

## REGULATING PRIVACY IN PUBLIC/PRIVATE SPACE: THE CASE OF NURSING HOME MONITORING LAWS

*Karen Levy  
Lauren Kilgour  
Clara Berridge*

*The emergence of consumer-purchased monitoring devices in shared, intimate spaces presents new challenges to privacy and its protection. Web-enabled video cameras, which allow family members to monitor one another in the name of care, are among the most prevalent technologies in this vein. These cameras have recently gained traction for remote monitoring of vulnerable relatives in nursing homes, where they are intended to detect and deter abuse and neglect in residents' rooms. But in so doing, cameras can create new privacy vulnerabilities for residents (many of whom have dementia and lack capacity for consent), frontline care workers, roommates in shared rooms, and others. State policymakers are grappling with these issues as they craft laws governing electronic monitoring in these complex public/private spaces, in which policymakers must balance competing – and sometimes irreconcilable – privacy and security interests.*

---

Karen Levy is an Assistant Professor, Department of Information Science, Cornell University and Associated Faculty, Cornell Law School.

Lauren Kilgour is a Ph.D. Candidate, Department of Information Science, Cornell University.

Clara Berridge is an Assistant Professor, School of Social Work, University of Washington.

The authors gratefully acknowledge the Borchard Foundation Center on Law and Aging for its generous support of this research. We thank Helen Nissenbaum, Bryce Newell, D.R. Jones, Scott Skinner-Thompson, Mary Madden, and participants in the 2017 Privacy Law Scholars Conference and the International Association for Gerontology and Geriatrics' 2017 World Congress for helpful feedback, and Trinh Le and Kim Lee for valuable research assistance.

*This Article presents a comparative analysis of seven state regimes that regulate the use of monitoring systems in nursing home resident rooms. We find that states attempt to protect privacy through a variety of interlocking privacy constraints: social, technical, and institutional safeguards that restrict how monitoring devices can be introduced and operated. Further, we map key relationships within which stakeholders hold specific privacy interests vis-à-vis one another, and describe how legal regimes do (and do not) address such interests. We consider implications for how privacy is conceptualized and regulated in multi-relational social contexts, in which the privacy and security interests of particular stakeholders necessarily impact those of others.*

\* \* \*

In 2017, Mary Ann Papp—a seventy-five-year-old resident of Neilson Place, a nursing home in Bemidji, Minnesota—developed a serious infection on her foot.<sup>1</sup> Mary Ann’s daughter, Lisa Papp-Richards, became concerned that Neilson Place staff may not have been taking adequate care of her mother and that they were unresponsive to her concerns.<sup>2</sup> So Lisa did something that is becoming increasingly common practice among families across the country: she went to Target, bought a \$199 surveillance camera, and installed it in her mother’s room.<sup>3</sup>

According to a complaint the Papps eventually filed with the Minnesota Department of Health, Neilson Place staff made clear that the camera was an unwelcome intrusion.<sup>4</sup> The staff reportedly unplugged the camera and would turn it away from her mother’s bed when they were caring for her. (Papp’s son-in-law later bolted the camera to the furniture.<sup>5</sup>) Eventually, the legality of the device was called into question:<sup>6</sup> should Lisa Papp-Richards be permitted to remotely monitor her mother’s room in a state facility? Or did countervailing factors—including the intimacy of the care that nursing home residents receive, the shared nature of the space, and employees’ own privacy interests—counsel against such recording?

The camera in Mary Ann Papp’s room is one instance of a much broader phenomenon: the massive expansion of the market for devices that collect data in the name of care. From pet cams to baby monitors, a

---

1. Chris Serres, *Minnesota Surveillance Camera Ruling a Victory for Nursing Home Residents*, STARTRIBUNE (May 23, 2017, 10:35 PM), <https://www.startribune.com/minnesota-maltreatment-finding-is-a-victory-for-granny-cams/423931753/>.

2. *Id.*

3. *Id.*

4. *See id.*

5. *Id.*

6. *Id.*

wide variety of “smart” consumer products are designed and sold to help people manage their closest and most intimate relationships.<sup>7</sup> In the best cases, these technologies can promote peace of mind and help anxious family members keep tabs on one another’s health and well-being, even at a distance. Cameras can be valuable tools for families overstretched by the labor of care, particularly when a family member is vulnerable due to illness or disability.

Among the most common technologies in this category are web-enabled video cameras, which allow family members to “peek in” on other family members remotely. These cameras have recently gained traction as a tool for families to remotely monitor elder relatives in long-term care institutions, like nursing homes and assisted living communities. Family members who are worried about potential abuse, neglect, or poor quality of care in residential settings may place hidden cameras in a family member’s room to confirm their suspicions or conspicuously place a camera in an attempt to deter abusive actions.

To be sure, the use of so-called “granny cams” is often motivated by an ethic of care and well-intentioned concern by family members. But these devices also raise important and novel issues about the privacy interests of the monitored.<sup>8</sup> Care in nursing home facilities is extremely intimate: residents often require assistance with activities of daily living that include dressing, bathing, and toileting.<sup>9</sup> Further, the vulnerability that engenders the need for care can also reduce personal autonomy and capacity for consent.<sup>10</sup> Monitoring technologies that aim to safeguard residents against perceived threats to health and safety

---

7. See, e.g., Josh Jones, *George Orwell Predicted Cameras Would Watch Us in Our Homes; He Never Imagined We’d Gladly Buy and Install Them Ourselves*, OPEN CULTURE (Nov. 28, 2017), <http://www.openculture.com/2017/11/george-orwell-never-imagined-wed-gladly-buy-and-install-cameras-in-our-homes.html> [hereinafter Jones]; Wilson Rothman, *Want to Spy on Your Children? Call it Monitoring . . . and Get Their Blessing*, WALL ST. J. (Aug. 30, 2017, 1:28 PM), <https://www.wsj.com/articles/want-to-spy-on-your-children-call-it-monitoring-and-get-their-blessing-1504114131>.

8. See, e.g., Clara Berridge, *Selling Passive Monitoring to Manage Risk in Independent Living: Frontline Workers in a Bind*, in UNDER OBSERVATION: THE INTERPLAY BETWEEN EHEALTH AND SURVEILLANCE 73 (Samantha Adams et al., eds. 2017); Clara Berridge, *Breathing Room in Monitored Space: The Impact of Passive Monitoring Technology on Privacy in Independent Living*, 56 THE GERONTOLOGIST 807 (2016); Luke Stark & Karen Levy, *The Surveillant Consumer*, 40 MEDIA, CULTURE, & SOC’Y 1202, 1208–09 (2018) [hereinafter Stark & Levy].

9. Brent C. Williams et al., *Activities of Daily Living and Costs in Nursing Homes*, NAT’L INST. OF HEALTH (1994), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4193443/>.

10. See *id.*

can, in so doing, create their *own* threats to their autonomy and well-being. What's more, these cameras can also implicate the privacy and security interests of third parties, including care workers, roommates, and visitors<sup>11</sup> in intimate spaces – as well as the institutions themselves.

These multivalent privacy dynamics create a complicated space for law. Minnesota, where Mary Jane Papp lives, lacks a statute specifically addressing the use of cameras in nursing home resident rooms, as do the vast majority of states; only seven states have specific rules on the books. In May 2017, the Minnesota Department of Health ruled in favor of the Papp family's right to use a camera in Mary Jane Papp's room – the first ruling to affirm such a right.<sup>12</sup> It sends the message that absent state laws to the contrary, families can use cameras to monitor a loved one's room without fear of retaliation from the facility.

The approaches taken by states that do regulate camera use can reveal quite a bit about how privacy is legally conceptualized in the nursing home environment. Given the complexity of the interests at stake, how are states balancing these factors in their policies? How do these balances reflect and weigh competing privacy and security interests of stakeholders, taking into account their unique needs and vulnerabilities? These interests include, among others:

- residents' interests in privacy, dignity, and physical and psychological well-being;
- the likelihood of diminished capacity for consent or awareness of cameras;
- families' legitimate interests in the protection and well-being of their relatives;
- facilities' interests in avoiding liability and ensuring compliance; and
- the privacy interests of nursing home workers (many of whom are themselves socioeconomically vulnerable).

In this Article, we undertake a comparative analysis of the state laws and regulations governing resident-room cameras in nursing homes. We focus on how such rules approach and balance the privacy concerns of the multiple relations involved in such contexts, and how legal protections do – and do not – address relationship-specific inter-

---

11. See Alex B. Lipton, *Privacy Protections for Secondary Users of Communications-Capturing Technologies*, 91 N.Y.U. L. REV. 396 (2016).

12. James M. Berklan, *Family Wins Camera Case*, MCKNIGHT'S LONG-TERM CARE NEWS (July 6, 2017), <http://www.mcknights.com/news/family-wins-camera-case/article/671588/>.

ests. Part I describes the relational and interdependent nature of privacy in public/private spaces. Part II describes in more detail the nursing home setting and the unique vulnerabilities that arise therein. In Part III, we describe the data and methods underlying our analysis. Part IV presents a taxonomy of sociotechnical privacy constraints in state nursing home camera laws, and Part V undertakes a relational mapping to understand how such constraints map onto the complex relationships in the space. In Part VI, we describe the implications of our study for understanding privacy regulation more generally.

## I. Relational and Interdependent Privacy in Public/Private Spaces

Privacy dynamics are inherently *relational*. Our vulnerabilities to privacy invasions depend on the nature of our specific relationships to other people, and vary by the degree of trust, behavioral norms, and expectations of duty and care that characterize a given relation. Information we intend to keep concealed from one party may not be particularly sensitive with respect to another—and as a result, the nature of the privacy protections we put in place may well differ in different relationships.

At the forefront of scholarship on this topic is Helen Nissenbaum's contextual integrity framework, which assesses privacy violations by considering whether information transmitted in a particular way—between particular actors, acting in specific relational roles—violates expected norms within a given context.<sup>13</sup> Other scholarship has clarified the fact that privacy expectations and desires depend on the parties *against whom* we desire privacy,<sup>14</sup> and has explained how delineated data-sharing expectations within social relationships help to define, maintain, and differentiate those relationships.<sup>15</sup>

At the same time, privacy is socially *interdependent*. Monitoring within one relationship oftentimes impacts relationships among associated parties—by creating new forms of risk, chilling certain types of behavior, and otherwise creating or complicating social dynamics

---

13. See HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* (2009) [hereinafter NISSENBAUM].

14. See Laurent Sacharoff, *The Relational Nature of Privacy*, 16 LEWIS & CLARK L. REV. 1249 (2012).

15. See Karen Levy, *Relational Big Data*, 66 STAN. L. REV. ONLINE 73 (2013).

within a setting.<sup>16</sup> Recent scholarship on networked privacy<sup>17</sup> and privacy externalities<sup>18</sup> further underscores the fact that information transmissions within dyads often echo outward, implicating the interests of third parties to the exchange.

These characteristics of privacy—its relationalism and its interdependence—become especially acute when information transmission occurs in physical spaces where both public and private interests are at stake. Nursing homes are a prime example of such a setting. A nursing home is a unique, hybrid space in which state interests and intimate activities are closely entwined. While nursing home rooms are intimate sites in which some of the most vulnerable residents live and are cared for—giving rise to strong privacy interests—they are also very closely regulated by states, which have tremendous authority to structure day-to-day living, and their own interests to protect (including the prevention of mistreatment and the limitation of liability). Privacy is interdependent in this context because, as we shall describe, decisions about one party's privacy can directly implicate the privacy interests of others in the space—and it is relational, in that information is differentially sensitive *as to* different parties who occupy and move within the space. Electronic monitoring in nursing homes, and the rules that regulate it, thus enter a particularly fraught context, in which the aims and targets of privacy protection, and the perceived threats thereto, are multivalent and interact in complex ways.

No federal law regulates the use of in-room cameras in nursing homes, and there is virtually no research on the effects or desirability of electronic monitoring in nursing home resident rooms to detect or deter abuse.<sup>19</sup> However, a number of states have statutes, regulations, or guidelines in force that explicitly permit private individuals to use

---

16. See Karen Levy & Solon Barocas, *Refractive Surveillance: Monitoring Customers to Manage Workers*, 12 INT'L J. OF COMM. 1166 (2018) [hereinafter Levy & Barocas]; see also DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 47-52 (2011) (explaining the limitations of understanding privacy as merely an individually-held right).

17. See Alice E. Marwick & danah boyd, *Networked Privacy: How Teenagers Negotiate Context in Social Media*, 16 NEW MEDIA & SOC'Y 1051 (2014).

18. See Joshua Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L. J. 385 (2015); Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 61/S J. L. & POL'Y INFO. SOC'Y 425 (2011).

19. Clara Berridge, Jodi Halpern, and Karen Levy, *Cameras on Beds: The Ethics of Surveillance in Nursing Home Rooms*, AM. J. BIOETHICS: EMPIRICAL BIOETHICS (forthcoming, on file with author) [hereinafter *Cameras on Beds*].

monitoring cameras in nursing facility resident rooms and place restrictions on doing so.<sup>20</sup>

These rules take a number of different approaches in balancing the privacy interests of various stakeholders. The rules differ in terms of how they provide notice of data collection, and to whom such notice is provided; what processes for consent are contemplated; what safeguards are required for data security and access; and many other features. Most fundamentally, taking a critical look at these laws helps us to understand who is perceived as posing privacy threats, what sorts of vulnerabilities are contemplated with respect to those threats, and how those vulnerabilities are protected. More broadly, doing so provides insight into how law might intersect with the design of connected devices in order to safeguard privacy in complex social settings.<sup>21</sup> The following section provides context about the issues at stake in nursing homes.

## II. Nursing Home Residents' Vulnerabilities to Abuse and Neglect

One among many quality-of-care concerns in nursing homes in the United States is the potential for abuse and neglect of residents. The media feature stories about elder abuse in long-term care facilities far more often than elder abuse that takes place within private homes—potentially leading to public perceptions that abuse is more common in

---

20. States with laws and regulations in force are Illinois, Louisiana, New Mexico, Oklahoma, Texas, Washington, and Utah. A few states have related guidelines, but no law: California, for example, has guidelines for facility-initiated camera use in assisted living facilities, and Maryland has guidelines for nursing centers if they choose to allow individuals to install cameras. 210 ILL. COMP. STAT. 32/1 (2011); LA. STAT. ANN. § 40:1193.1 (2018); N. M. STAT. ANN. § 24-26-21 (2018); OKLA. STAT. titl 63, § 1-1953.1 (2018); TEX. HEALTH & SAFETY CODE ANN. § 555.025 (2017); UTAH CODE ANN. § 26-21-301 (LexisNexis 2018); WASH. ADMIN. CODE § 388-97-0380 (2017); Office of Health Care Quality, *Guidelines for Electronic Monitoring*, MD. DEP'T OF HEALTH & MENTAL HYGIENE (Dec. 1, 2003), <https://dhmh.maryland.gov/ohcq/ltc/docs/reports/149report.pdf>; *Reference Materials for Office Functions*, CAL. OFF. OF SOC. SERVICES (Aug. 2015), <http://www.cclld.ca.gov/res/pdf/OfficeFunctions.pdf>.

21. See generally WOODROW HARTZOG, *PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES* (2018); M. Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012) [hereinafter Calo]; Meg Leta Jones, *Privacy Without Screens and the Internet of Other People's Things*, 51 IDAHO L. REV. 639 (2015).

residential facilities than in private homes.<sup>22</sup> There are no reliable estimates of abuse or neglect in nursing homes,<sup>23</sup> but the prevalence of physical, psychological, or sexual abuse, neglect, or financial exploitation across all settings is estimated at about 10% of older adults in the United States.<sup>24</sup> Nursing home residents are known to have been subject to cyberbullying and harassment, whereby staff have been caught disseminating intimate and embarrassing photos and videos of residents from their mobile devices.<sup>25</sup> On the whole, nursing home residents are considered more vulnerable than other older adults, as they have greater impairments and may be subject to abuse at the hands of staff as well as fellow residents.<sup>26</sup> Approximately half (50.4%) of nursing home residents in the United States have Alzheimer's disease or related dementias,<sup>27</sup> and abuse is thought to be dramatically underreported among those with cognitive impairment.<sup>28</sup>

By law, nursing homes are charged with the protection of their residents;<sup>29</sup> however, the incentive structure for the internal report of abuse is weak, and many factors complicate the sanctioning or closure of poor-quality nursing facilities.<sup>30</sup> The Nursing Home Reform Act of

---

22. Teresa Mastin et al., *Newspapers' Framing of Elder Abuse: It's Not a Family Affair*, 84 JOURNALISM & MASS COMM Q. 777 (2007).

23. Lisa M. Gibbs & Laura Mosqueda, *Confronting Elder Mistreatment in Long-Term Care*, 12 ANNALS OF LONG-TERM CARE 30 (2004) [hereinafter Gibbs & Mosqueda]; Mark S. Lachs & Karl A. Pillemer, *Elder Abuse*, 373 NEW ENG. J. MED. 1947, 1950 (2015) [hereinafter Lachs].

24. Ron Acierno et al., *Prevalence and Correlates of Emotional, Physical, Sexual, and Financial Abuse and Potential Neglect in the United States: The National Elder Mistreatment Study*, 100 AM. J. PUB. HEALTH 292, 292 (2010) [hereinafter Acierno et al.].

25. Memorandum from the Ctrs. For Medicare & Medicaid Servs. On Protecting Resident Privacy and Prohibiting Mental Abuse Related to Photographs and Audio/Video Recordings by Nursing Home Staff to State Survey Agency Directors 16-33 (Aug. 5, 2016), <https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Downloads/Survey-and-Cert-Letter-16-33.pdf>.

26. INST. OF MED. & NAT'L RES. COUNCIL, ELDER ABUSE AND ITS PREVENTION: WORKSHOP SUMMARY (2014); Gibbs & Mosqueda, *supra* note 23.

27. Lauren Harris-Kojetin et al., *Long-Term Care Providers and Services Users in the United States: Data from the National Study of Long-Term Care Providers, 2013-2014*, 3 VITAL & HEALTH STAT. 1, 40 (2016).

28. *Research*, NAT'L CTR. ON ELDER ABUSE, <https://ncea.acl.gov/whatwedo/research/statistics.html#14> (last visited Oct. 17, 2018).

29. Joshua M. Wiener, *An Assessment of Strategies for Improving Quality of Care in Nursing Homes*, 43 THE GERONTOLOGIST 19, 20 (2003) [hereinafter Wiener].

30. *Id.*

1987<sup>31</sup> was passed in response to concerns about abuse, neglect, and inadequate care in nursing homes. The law applies to facilities that receive Medicare or Medicaid payment, the funding source for about three-quarters of nursing home residents.<sup>32</sup> It specifies a range of rights for residents, including the freedom from “abuse, neglect, misappropriation of resident property, and exploitation.”<sup>33</sup> In addition to protection from abuse, regulations promulgated under the Act delineate a right to “personal privacy” for residents of nursing homes, applicable to the resident’s “accommodations, medical treatment, written and telephone communications, personal care, visits, and meetings of family and resident groups[.]”<sup>34</sup> The Social Security Act mandates federal standards for facilities,<sup>35</sup> and the Centers for Medicare and Medicaid Services (“CMS”) oversee the federal certification of compliance that must be conducted by state agencies through annual, unannounced surveys of facilities.<sup>36</sup> States also have the option of setting additional standards.<sup>37</sup>

Sanctions for facilities that do not meet these standards are, in practice, difficult to impose because nursing homes effectively hold residents “hostage.” Financial sanctions can further restrict payment on staffing, and closure and resident relocation are extremely difficult situations for residents and their families.<sup>38</sup> The financial and political barriers to further strengthening federal regulations on nursing homes are formidable, in part because additional government funding would be required given the significant role of government programs like Medicaid and Medicare.<sup>39</sup>

This impasse in strengthening regulatory protections has contributed to the increasing *privatization* of the protection of nursing home

---

31. 42 U.S.C. §1396r (2012).

32. Wiener, *supra* note 29, at 20.

33. 42 C.F.R. § 483.12 (2018). Among other implementing regulations of the Nursing Home Reform Act, this regulation guarantees nursing home residents these freedoms, and requires that facilities institute policies and procedures to prohibit, prevent, and remediate such mistreatment.

34. 42 C.F.R. § 483.10 (2018).

35. 42 U.S.C. § 1395i (2012).

36. *Nursing Homes* (2018), CENTERS FOR MEDICARE & MEDICAID SERVICES, <https://www.cms.gov/medicare/provider-enrollment-and-certification/certificationandcompliance/nhs.html> (last updated Sept. 20, 2018, 9:04 AM).

37. *Id.*

38. Wiener, *supra* note 29, at 21.

39. *Id.*

residents. One approach is increased consumer empowerment, including consumer advocacy—such as ombudsman programs and the provision by CMS of information to consumers about facilities—in the hope of improving the choices consumers make in an ostensible free market for selecting facilities in which to house their loved ones.<sup>40</sup> The CMS Nursing Home Compare website<sup>41</sup> makes a range of information available to the public, including citations facilities have received for care deficiencies.<sup>42</sup> In addition, independent advocacy groups lobby and provide public education about quality of care in nursing homes.<sup>43</sup>

However, the efficacy of the consumer empowerment approach is questionable. Consumer advocacy and increased access to information can be undermined when basic assumptions do not hold, such as the idea that family members of nursing home residents have time for advocacy work, or that they have multiple facilities to choose from within driving distance for regular visits.<sup>44</sup> Nursing home placement is often triggered by rapid events, such as a fall or other health change, which leaves families with little time to educate themselves about facilities when a loved one needs to move.<sup>45</sup> Despite its limitations, there has been a recent trend towards consumer empowerment in nursing home care,<sup>46</sup> which is further reflected in the use of in-room cameras by family members.

The use of cameras in nursing home residents' rooms is not new, but public interest in the topic is renewed periodically—particularly when the media highlight a disturbing case of abuse committed by a

---

40. *Id.* at 24.

41. *Nursing Home Compare*, MEDICARE.GOV, <https://www.medicare.gov/nursinghomecompare/search.html> (last visited Oct. 17, 2018).

42. *Id.*

43. For example, California Advocates for Nursing Home Reform (CANHR), a nonprofit operating since 1983, works toward “improving the choices, care and quality of life for California’s long term care consumers” and describes its goal as “educat[ing] and support[ing] long term care consumers and advocates regarding the rights and remedies under the law . . . .” *About CANHR*, CAL. ADVOCATES FOR NURSING HOME REFORM, <http://www.canhr.org/about/index.html> (last visited Oct. 17, 2018).

44. Wiener, *supra* note 29, at 23.

45. *Id.*

46. Nicholas G. Castle & Jamie C. Ferguson, *What Is Nursing Home Quality and How Is It Measured?*, 50 *THE GERONTOLOGIST* 426, 437 (2010); Wiener, *supra* note 29.

staff member and captured by a camera in a resident's room.<sup>47</sup> The driving imperative for (covert and overt) use of cameras in resident rooms is the specter of abuse, neglect, and exploitation. Family members may not trust that the facility is safeguarding residents and their belongings. The increased use of cameras can be read as a displacement of responsibility for resident safety in these spaces from the state to residents and their family advocates. As a result of this practice, states and some individual facilities are beginning to create their own policies for such use of in-room cameras.<sup>48</sup> Notably, in taking this market-driven approach to resident safety, states and facilities institutionalize privacy and security protections that impact *only* those residents who have family advocates, and the technical, social, and financial wherewithal to install and monitor cameras and the data they gather.

In 2016, one of this Article's authors—Dr. Berridge—conducted an online survey to learn about nursing center and assisted living policies and current use of cameras in resident rooms.<sup>49</sup> The 273 respondents, all administrators and other employees working in nursing and assisted living facilities, were asked to write in both their chief concerns and potential advantages of camera use in resident rooms.<sup>50</sup> By far, the most common issue noted, among both concerns and advantages, was the potential for the violation of resident, roommate, visitor, or staff privacy, followed by concern for residents' dignity.<sup>51</sup>

Respondents further noted the inability to gain roommates' consent when family members use covert surveillance, and the difficulty of ascertaining if a resident with dementia would want a camera that their legal representative wants to use.<sup>52</sup> As noted, reduced capacity is common among nursing home residents—and these residents are less able to report abuse or neglect; when they do report such maltreatment,

---

47. See, e.g., Paula Span, *In Nursing Homes, Eyes that Never Turn Away*, N.Y. TIMES (Oct. 8, 2014, 12:53 PM), <http://newoldage.blogs.nytimes.com/2014/10/08/in-nursing-homes-eyes-that-never-turn-away/>.

48. See *Cameras on Beds*, *supra* note 19.

49. *Id.*

50. *Id.*

51. *Id.*

52. See generally Alistair R. Niemeijer et al., *Ethical and Practical Concerns of Surveillance Technologies in Residential Care for People with Dementia or Intellectual Disabilities: An Overview of the Literature*, 22 INT'L PSYCHOGERIATRICS 1129 (2010).

their reports may not be considered valid.<sup>53</sup> Therefore, these are the residents for whom family members are *most* likely to turn to cameras, and the *least* likely to be able to actively participate in decisions about being placed on camera.

The survey respondents also frequently emphasized the potential for cameras to demoralize the certified nursing assistants (“CNA”) who provide the most frequent and intimate frontline care to residents.<sup>54</sup> They worried that being made to work on camera would communicate mistrust, have a chilling effect on care relationships, and contribute to the problem of low-quality jobs and poor retention.<sup>55</sup> The majority of this difficult work is performed by women of color (including Black, Filipina, and Latina women); over one-third are Black or African American.<sup>56</sup> CNAs receive little training<sup>57</sup> and have an injury rate 3.5 times that of the typical U.S. worker.<sup>58</sup> Their median hourly wage is \$11.87, with annual income averaging \$19,000, and turnover rates are high (estimates range widely from 43% to 86%).<sup>59</sup> The high turnover rates contribute to the pervasive problem of understaffing, which itself poses a range of additional quality and safety risks.<sup>60</sup>

It is into this breach of conflicting interests and vulnerabilities that states have begun to articulate rules governing camera use. Part III analyzes how they have done so.

---

53. Catherine Hawes, *Elder Abuse in Residential Long-Term Care Settings: What is Known and What Information is Needed?*, in *ELDER MISTREATMENT: ABUSE, NEGLECT, AND EXPLOITATION IN AN AGING AMERICA* 446, 446 (R. Bonnie & R. Wallace, eds., 2003).

54. See *Cameras on Beds*, *supra* note 19.

55. *Id.*

56. *U.S. Nursing Assistants Employed in Nursing Homes: Key Facts*, PHI (2016), <https://phinational.org/wp-content/uploads/legacy/phi-nursing-assistants-key-facts.pdf>.

57. *Id.*

58. *Id.*

59. Nicholas G. Castle & John Engberg, *Staff Turnover and Quality of Care in Nursing Homes*, 43 *MED. CARE* 616 (2005); *2012 Quality Report*, AM. HEALTH CARE ASS'N (2012), [http://www.ahcancal.org/quality\\_improvement/Documents/AHCA%20Quality%20Report%20FINAL.pdf](http://www.ahcancal.org/quality_improvement/Documents/AHCA%20Quality%20Report%20FINAL.pdf).

60. Wiener, *supra* note 29, at 22-23.

### III. Examining Privacy Protections in In-Room Camera Laws: Data and Methods

In order to assess how privacy is conceptualized and balanced in these contexts, we conducted a comparative sociolegal study of relevant legislation in U.S. states. This analysis proceeded in two stages. First, we identified and collected all active state-level laws and regulations governing in-room camera use in nursing homes.<sup>61</sup> The states with rules in force that govern in-room camera use are Texas (which passed legislation in 2001),<sup>62</sup> New Mexico (2004),<sup>63</sup> Washington (2008),<sup>64</sup> Oklahoma (2013),<sup>65</sup> Illinois (2015),<sup>66</sup> Utah (2016),<sup>67</sup> and Louisiana (2018).<sup>68</sup>

After we assembled a collection of statutes and regulations, we conducted comparative qualitative coding of the dataset, noting in particular attributes like key substantive distinctions within camera policies (for example, rules about consent, data retention, usage, and data transfer), how different rules conceptualize and address privacy-related and other interests of different stakeholders, and how rules evidence multiple conceptions of the affordances of electronic monitoring equipment. Our initial coding scheme was inductive, though substantially informed by our prior research (including Dr. Berridge's survey results). Two members of the research team independently coded the dataset, refined the codes, and iteratively re-coded for analysis.

---

61. In addition to nursing homes, some states have extended their statutes and regulations to govern camera use in assisted living facilities, as well. Camera use in assisted living facilities is likely to become a more prevalent concern due to the dramatic growth of this facility type. David C. Grabowski et al., *Assisted Living Expansion and the Market for Nursing Home Care*, 47 HEALTH SERVICES RES. 2296, 2297 (2012). Texas and Utah's nursing home laws also cover assisted living communities. Lois A. Bowers, *Utah camera bill headed to governor's desk*, MCKNIGHT'S SENIOR LIVING (Mar. 3, 2016), <http://www.mcknightsseniorliving.com/news/utah-camera-bill-headed-to-governors-desk/article/481094/>. However, our present inquiry focuses on nursing homes specifically – in part because they are more stringently regulated than assisted living facilities, and in part to create a more consistent basis for comparison among privacy protections therein. Future research might consider the role of differences in institution type when assessing the means and effectiveness of privacy protections.

62. TEX. HEALTH & SAFETY CODE ANN. §§ 242.841–242.852 (West 2017).

63. N.M. STAT. ANN. §§ 24-26-1–24-26-12 (West 2017).

64. WASH. ADMIN. CODE §§ 388-97-0380–388-97-0400 (2017).

65. OKLA. STAT. ANN. tit. 63, §§ 1-1953.1–1953.7 (West 2017).

66. 210 ILL. COMP. STAT. 915, 32/1–32/99 (2017).

67. UTAH CODE ANN. §§ 26-21-301–26-21-305 (West 2016).

68. LA. STAT. ANN. §§ 40:1193.1–1193.11, 2010.8 (2018).

Based on these descriptive codes, we undertook two stages of analysis. First, we delineated the mechanisms through which states have attempted to regulate camera use in resident rooms, and categorized them thematically based on *how* they attempted to address privacy concerns. These categories form the basis of our taxonomy of sociotechnical strategies (which we term *constraints*) described in Part IV. The goal of this analysis is to investigate the “toolkit” of approaches available in law for the protection of privacy within the nursing home setting—including technical, social, and institutional forms of regulation.

In the second stage of our analysis, we shift our focus to relationships, asking *for whom* and *against whom* privacy is protected. We created a network map of each interpersonal and institutional relationship among key stakeholders, and articulated the core privacy, security, and information transmission concerns that characterize each relation. We selected five dyads of primary interest. For each of these five relationships, we considered how the sociotechnical privacy constraints instantiated in the law attempt to mediate how information flows and functions therein—and which concerns seem to be *unaddressed* in the law. Our analysis here is informed by Nissenbaum’s contextual integrity framework and its recognition of the importance of roles and relationships in understanding privacy violations. It further considers how the transmission of information within one relationship can have effects on other actors in complex social environments. The goal of this analysis is to consider how the current legal landscape prioritizes and balances among the interests of multiple actors in the space, including monitored residents, their family members and roommates, care workers, and the facilities themselves. This analysis comprises Part V.

#### **IV. How is Privacy Protected? Forms of Privacy Constraint**

Each of the statutes and regulations we considered has a common general purpose: to regulate the installation and use of in-room monitoring devices<sup>69</sup> by a resident or her representative. Each measure explicitly permits the installation and use of such devices under certain

---

69. The terminology that states use to describe the technologies at issue varies. The statutory and regulatory schemes in our dataset use either the broad term “electronic monitoring” or “monitoring device” throughout, and subsequently define such monitoring devices by their capabilities (primarily video and/or audio data

delineated conditions; each further clarifies that the installation and use of monitoring equipment must occur at the resident's own expense.

But despite this common purpose, the rules we analyzed varied significantly in terms of the means through which they regulated and balanced privacy interests. States regulate privacy in nursing homes by implementing a wide variety of *constraints* on camera use. We identified and categorized these forms of constraint based on *how* they attempted to protect the privacy and security of stakeholders: by delimiting the capture and transmission of data, by providing notice of the same, by ensuring consent, by limiting visibility, and the like. For instance, by positioning a camera to restrict its field-of-capture (a spatial constraint) and limiting the permissible hours when a device can record (a temporal constraint), a law might seek to confine what data might be gathered, and about whom. By mandating the placement of signage outside a room with a camera (a visual constraint) and requiring consent forms before camera installation (a bureaucratic constraint), a law might seek to provide notice of such recording to interested parties.

The breadth of constraints we found in states' rules demonstrates a wide range of ways that privacy and its protection can be conceptualized in this multi-stakeholder setting. However, the constraints can be taxonomized according to thematic types for analytic clarity, as illustrated in the table below. The following section describes the general contours of each constraint category.

---

capture, typical of a video camera; we expand on differences in data capture constraints in Part IV.B., *infra*). It is clear from the definitions of these statutes and regulations that cameras are the primary technology intended to be regulated. In this article, we use the terms "electronic monitoring," "monitoring device," and "camera" interchangeably, to refer to the class of devices governed by the statutes and regulations in our dataset.

Table 1: Types of Privacy-Related Constraint in Nursing Home Camera Rules

<b>Bureaucratic constraints</b>	Required consent forms to be tendered to facility and state Rules against institutional retaliation State sanctions against noncompliant nursing homes
<b>Technological constraints</b>	Hardware specifications Constraints on collection of certain data types Restrictions on precision (focus, volume, etc.) Rules against tampering with equipment
<b>Visual constraints</b>	Placement of signs and notices Conspicuous placement of monitoring equipment
<b>Spatial constraints</b>	Positioning of cameras Reconfiguration of rooms Permitting residents to move rooms to accommodate privacy preferences
<b>Temporal constraints</b>	Restricted hours of operation Rules about duration and re-evaluation
<b>Situational constraints</b>	Requirement of perceived threat before recording is permitted Restrictions on recording for health care visits, financial matters, religious matters, etc. General state laws protecting residents' dignity and autonomy
<b>Litigation constraints</b>	Limitations on admissibility and authentication of recordings Limitations on liability Rules about when recordings are deemed "seen" in abuse complaints

#### A. Bureaucratic Constraints

All states in our dataset mediated parties' privacy interests through mandated procedures regarding how nursing homes must act with respect to in-room camera use. Each state has detailed rules regarding approval and consent processes, paperwork that must be filed, and the like. These processes function as *bureaucratic* constraints which operate toward a number of ends: they serve to enable residents (or their family members)<sup>70</sup> to monitor their rooms, to establish consent

---

70. As we discuss in more detail in Part V.A., residents and their family representatives may have quite different (and potentially incompatible) monitoring preferences, giving rise to concerns about how camera use impacts privacy *between* these two parties. However, in most cases, the statutory and regulatory text makes little distinction between the two parties.

from roommates, and to prevent nursing homes from retaliating against residents when they or their family members wish to install cameras.

Each of the statutory schemes in our dataset requires *written notification and consent forms*.<sup>71</sup> Some states require nursing homes to inform residents in writing of their rights to conduct monitoring,<sup>72</sup> and to limit in-room monitoring only to cases of resident request and consent.<sup>73</sup> Concomitantly, all states in our dataset had procedures by which residents or their representatives had to notify facilities, in writing, of their intent to conduct monitoring;<sup>74</sup> in addition, all states required written consent to camera use by a resident's roommates<sup>75</sup> (or, in some cases, the roommates' legal representatives<sup>76</sup>).

Five states in our dataset have rules preventing nursing homes from *retaliating* against residents or family members who wish to install and use cameras in their rooms; these rules hold, generally, that facilities may not discharge or deny admission to a resident who chooses to monitor their room electronically, or whose legal representative does so.<sup>77</sup> In addition, some rules established state-level sanctions against nursing homes that fail to comply with residents' rights regarding electronic monitoring.<sup>78</sup>

---

71. The only exception to this is *covert* monitoring, permitted in Texas only. See discussion *infra* Parts V.B. and V.E.

72. See, e.g., OKLA. STAT. ANN. tit. 63, § 1-1953.2(A) (West 2017).

73. WASH. ADMIN. CODE § 388-97-0400(1)(a) (2017).

74. 210 ILL. COMP. STAT. 32/20(a)-(b) (2017); LA. STAT. ANN. § 40:1193.6(2) (2018); N.M. STAT. ANN. § 24-26-3(A)(1) (West 2017); OKLA. STAT. ANN. tit. 63, § 1-1953.6(A)-(B) (West 2017); TEX. HEALTH & SAFETY CODE ANN. § 242.846(a) (West 2017); UTAH CODE ANN. § 26-21-303(1)(a) (West 2016); WASH. ADMIN. CODE § 388-107-0790(2)(c) (2017).

75. 210 ILL. COMP. STAT. 32/15 (2017); LA. STAT. ANN. § 40:1193.3(4) (2018); N.M. STAT. ANN. § 24-26-6(C) (West 2017); OKLA. STAT. ANN. tit. 63, § 1-1953.6(B) (West 2017); TEX. HEALTH & SAFETY CODE ANN. § 242.846(b)(3) (West 2017); UTAH CODE ANN. § 26-21-303(1)(b) (West 2016); WASH. ADMIN. CODE § 388-78A-2690(2)(c) (2017).

76. See, e.g., OKLA. STAT. ANN. tit. 63, § 1-1953.6(c)(2) (West 2017); see also N.M. STAT. ANN. § 24-26-6(c) (West 2017).

77. These states are Louisiana (LA. STAT. ANN. § 40:1193.8 (2018)), New Mexico (N.M. STAT. ANN. § 24-26-11 (West 2017)), Oklahoma (OKLA. STAT. ANN. tit. 63, § 1-1953.2(B) (West 2017)), Texas (TEX. HEALTH & SAFETY CODE ANN. § 242.847(d) (West 2017)), and Utah (UTAH CODE ANN. § 26-21-304 (West 2016)).

78. For instance, in Texas, the Department of Human Services can sanction and fine administrators of nursing homes who refuse to allow residents to conduct electronic monitoring or who retaliate against them. TEX. HEALTH & SAFETY CODE ANN. § 242.851(a) (West 2017); 40 TEX. ADMIN. CODE § 19.422(j) (2017).

## B. Technological Constraints

Each state specifies what *types of equipment* can be used for monitoring, and what *types of data* they may collect—with attention paid to requirements related to permissible hardware, technological and data-based affordances, and potential tampering with devices. The rules in each state allow for the use of audio or visual data collection, or both. Within these allowances, there is variation in terms of what types of monitoring devices are considered permissible, how they *may not* be installed and operated, and what forms of data they *may not* collect. For example, Illinois's statute does not “allow the use of an electronic monitoring device to take *still photographs*.”<sup>79</sup> Oklahoma, Illinois, Texas, and Utah bar the use of monitoring devices for nonconsensual interception of private communications, in accordance with broader anti-wiretapping regulations.<sup>80</sup>

Qualifications regarding *network-enabled devices* are also presented in four states.<sup>81</sup> In Illinois, the type of monitoring device(s) that residents are allowed to select explicitly *includes* units that “broadcast” activities and sounds that occur in the room.<sup>82</sup> New Mexico's regulation states that *if* the selected device “uses internet technology,” it must also “have at least 128-bit encryption and enable a secure socket layer (‘SSL’),”<sup>83</sup>—the only mention of data encryption provisions in our dataset. Louisiana's provision excludes devices that are “connected to the facility's [nursing home's] computer network.”<sup>84</sup> Utah has the strictest technological limitation in this regard, stating that monitoring devices covered by its law do *not* include “a device that is connected to the Internet or that is set up to transmit data via an electronic communication.”<sup>85</sup>

---

79. 210 ILL. COMP. STAT. 32/10(b) (2017) (emphasis added).

80. Illinois ((210 ILL. COMP. STAT. 32/10(b) (2017)), Oklahoma (OKLA. STAT. ANN. tit. 63, § 1-1953.1 (6) (West 2017)), Texas (TEX. HEALTH & SAFETY CODE ANN. § 242.841(2)(B) (West 2017)), and Utah (UTAH CODE ANN. § 26-21-303(3)(b) (West 2016)).

81. These states are: Illinois (210 ILL. COMP. STAT. 32/20(7)(b) (2017)), New Mexico (N.M. CODE R. 9.2.23.9(C) (LexisNexis 2017)), and Utah (UTAH CODE ANN. §26-21-302(3)(b)(ii) (West 2016)).

82. 210 ILL. COMP. STAT. 32/20(7)(b) (2017).

83. N.M. CODE R. 9.2.23.9(C) (LexisNexis 2017).

84. LA. STAT. ANN. § 40:1193.2(3)(a) (2018).

85. UTAH CODE ANN. § 26-21-302(3)(b)(ii) (West 2016). We interpret this provision to mean that residents may not select and install such a device, though strictly speaking, one might also interpret the statute as specifying that such devices are merely out of the scope of the provision.

The spectrum of permissibility related to network-enabled devices raises questions about the malleability of these laws in the face of rapid technological development. These controls suggest that buyers have the *option* of purchasing a monitoring device that is *not* network-enabled. It is increasingly difficult to obtain such a “disconnected” device. Furthermore, in Oklahoma and Texas, the statutes introduce conditions about how “tapes and recordings” collected by residents’ monitoring devices may be viewed, used, or transmitted.<sup>86</sup> References to “tapes” suggest that the law contemplated the use of increasingly rare device types.

Other states restrict the *precision* with which monitoring devices may collect data about their surroundings. New Mexico’s law allows a resident to establish “limits on the . . . focus or volume[] of a monitoring device” as a condition of use.<sup>87</sup>

Specific restrictions are also introduced to protect against *destruction, hampering, obstruction, and tampering* with devices. Illinois, New Mexico, Oklahoma, Texas, and Louisiana mandate that tampering with or intervening in the operation of authorized monitoring devices constitutes a criminal offense;<sup>88</sup> the offense category pertaining to such offenses varies.<sup>89</sup> New Mexico, Texas, and Louisiana’s criminalization of tampering relates to both the defilement of the monitoring device itself *as well as* the data or recording collected by the device.<sup>90</sup>

### C. Visual Constraints

Several states introduce *visual* restrictions on the installation and use of monitoring devices. This is attempted through two primary approaches: by requiring a form of *signage* alerting people about the use

---

86. OKLA. STAT. ANN. tit. 63, § 1-1953.1(1) (West 2017); TEX. HEALTH & SAFETY CODE ANN. § 242.841 (1) (West 2017).

87. N.M. STAT. ANN. § 24-26-3 (West 2017).

88. 210 ILL. COMP. STAT. 32/40(a)-(d) (2017); LA. STAT. ANN. § 40:1193.8(B)(1) (2018); N.M. CODE R. § 9.2.23.20 (LexisNexis 2017); OKLA. STAT. ANN. tit. 63, § 1-1953.3(a)-(b) (West 2017); TEX. HEALTH & SAFETY CODE § 242.852 (West 2017).

89. 210 ILL. COMP. STAT. 32/40(a)-(d) (2017) (classifying such offenses as class B misdemeanors); OKLA. STAT. ANN. tit. 63, § 1-1953.3(a)-(b) (West 2017) (classifying such offenses as misdemeanors punishable by a \$5000 fine).

90. Intentionally hampering, tampering, obstructing, or destroying a monitoring device and/or its *recording* are punishable as class 4 felonies in New Mexico (N.M. CODE R. 9.2.23.20 (LexisNexis 2017)), and as class B misdemeanors in Texas (TEX. HEALTH & SAFETY CODE ANN. § 242.852(a)-(b) (West 2017)); *see also* LA. STAT. ANN. § 40:1193.8 (B)(1).

of monitoring devices in residents' rooms (and in some cases further stipulating elements of the signs' content, placement, and maintenance); and by requiring *conspicuous placement* of the devices in rooms, presumably as a form of notice.

Several laws in our dataset state that a resident using an in-room monitoring device must (or in some cases, may) post a sign at or near the entrance to their room stating that a monitoring device is actively being operated within the room itself.<sup>91</sup> Four require that the notice or its placement be "conspicuous."<sup>92</sup> Some statutes indicate that signage requirements outside of the monitored room are optional, rather than mandatory: in Utah, facilities have discretion to require signage,<sup>93</sup> while in Oklahoma, the resident holds discretion to post a sign.<sup>94</sup> As we discuss *infra*, other states require posting at facility entrances.<sup>95</sup> Four states specifically mandate the textual content of the sign.<sup>96</sup>

---

91. Illinois (210 ILL. COMP. STAT. 32/30(b) (2017)); Louisiana (LA. STAT. ANN. § 40:1193.9(A) (2018)); New Mexico (N.M. CODE R. 9.2.23.18 (LexisNexis 2017)); Oklahoma (OKLA. STAT. ANN. tit. 63, § 1-1953.5 (B) (West 2017)); Texas (TEX. HEALTH & SAFETY CODE ANN. § 242.847 (West 2017)); Utah (UTAH CODE ANN. § 26-21-304(3) (West 2016)).

92. Illinois (210 ILL. COMP. STAT. 32/25(d) (2017)), Louisiana (LA. STAT. ANN. § 40:1193.9(A) (2018)), New Mexico (N.M. CODE R. 9.2.23.18 (LexisNexis 2017)), and Texas (TEX. HEALTH & SAFETY CODE ANN. § 242.847(b) (West 2017)).

93. UTAH CODE ANN. § 26-21-304(3) (West 2016) (emphasis added).

94. OKLA. STAT. ANN. tit. 63, § 1-1953.5 (B) (West 2017) (emphasis added).

95. See *infra* Part V.D. (resident-visitor dyad).

96. In Illinois, signs posted at facility entrances must read, "Electronic Monitoring: The rooms of some residents may be monitored electronically by or on behalf of the residents," and signs posted outside of resident rooms using monitoring devices must read, "This room is electronically monitored." 210 ILL. COMP. STAT. 32/30(a) (2017). Louisiana stipulates that the sign at the main entrance must read, "Electronic Monitoring. The rooms of some residents may be equipped with electronic monitoring devices installed by or on behalf of the resident" and that the sign outside the specific resident room must read "This room is electronically monitored" (LA. STAT. ANN. § 40:1193.9 (2018)). In New Mexico, the sign posted outside of a resident room using a monitoring device must read, "WARNING: THIS ROOM IS MONITORED ELECTRONICALLY." N.M. CODE R. 9.2.23.18 (LexisNexis 2017). New Mexico requires the language of the sign to be presented in English and Spanish. Texas prescribes "an 8-inch by 11-inch notice" that must "state in large easy-to-read type, 'The rooms of some residents may be monitored electronically by or on behalf of the residents. Monitoring may not be open and obvious in all cases.'" 40 TEX. ADMIN. CODE § 19.422(g) (2017). Texas mandates that signage must exist at main entrances warning entrants that some residents' rooms "may be" monitored, regardless of whether or not such monitoring is actively happening. TEX. HEALTH & SAFETY CODE ANN. § 242.850 (West 2017). Texas's provisions also go further to warn entrants that such monitoring is not necessarily open and obvious, which is the only mention throughout our dataset indicating that monitoring devices may not be immediately identifiable by entrants. *Id.*

Two states require the placement of in-room monitoring devices themselves to be *visibly perceptible*.<sup>97</sup> Illinois's statute states that the monitoring devices must be "placed in a conspicuously visible location in the room,"<sup>98</sup> Washington's regulations state that "the video camera [must be] clearly visible,"<sup>99</sup> and Texas's statute asserts that residents' monitoring devices must be in "plain view."<sup>100</sup> Such conspicuous placement presumably alerts entrants to the presence of a monitoring device and operates as a form of visceral notice<sup>101</sup> of surveillance.

#### D. Spatial Constraints

Several states' rules implemented *spatial* constraints for privacy protection. These fall into three general categories: provisions specifying the positioning of monitoring devices, provisions contemplating the reconfiguration of space around devices, and provisions specifying the positioning of people in relation to such devices. Illinois requires the *positioning of the device* to be set at the moment of its installation, allowing only for the use of "fixed position" cameras, as does Louisiana.<sup>102</sup> Other states do not mandate that devices be fixed, and suggest that cameras be routinely repositioned as a condition of consent to monitoring (e.g., by roommates, or in cases of specific visitors).<sup>103</sup> Louisiana also has a provision requiring that any renovations or alterations to "the structure of the resident's room . . . in order to accommodate a monitoring device" must be performed by a licensed contractor, demonstrating that *spatial reconfiguration* is contemplated as a means toward privacy protection.<sup>104</sup>

---

97. 210 ILL. COMP. STAT. 32/25(d) (2017); WASH. ADMIN. CODE §§ 388-76-10720(2)(c)(iii) (2017).

98. 210 ILL. COMP. STAT. 32/25(d) (2017).

99. WASH. ADMIN. CODE §§ 388-76-10720(2)(c)(iii), 388-78A-2680(2)(d)(iii), 388-97-0380(d)(iii), 388-107-0780(2)(c)(iii) (2017).

100. TEX. HEALTH & SAFETY CODE ANN. § 242.847 (West 2017).

101. Calo, *supra* note 21, at 1030 (describing visceral notice as "leverag[ing] a consumer's very experience of a product . . . to warn or inform" as a form of privacy disclosure, rather than depending on written descriptions of policies).

102. 210 ILL. COMP. STAT. 32/5 (2017); LA. STAT. ANN. § 40:1193.4(E) (2018).

103. See *infra* Part V.B. (resident-roommate dyad) and Part V.D. (resident-visitor dyad). For example, Oklahoma's statute permits consent to be conditioned on "the camera being pointed away from" a resident. OKLA. STAT. ANN. tit. 63, § 1-1953.6(D)(1) (West 2017).

104. LA. STAT. ANN. § 40:1193.3(B) (2018).

Other provisions provide that people, not devices, be the ones to move out of monitored space: as we discuss in more detail *infra*, residents in shared spaces who wish to go unmonitored may *change rooms* to move away from the device, and must be reasonably accommodated by the nursing home facility in so doing.<sup>105</sup>

### E. Temporal Constraints

Some states contemplate *temporal* limits on the operation of monitoring devices as a means of privacy protection. Three of the statutes in our dataset make specific reference to limitations on the *times of day* that a device may collect data.<sup>106</sup> For example, New Mexico requires that a resident “may establish and the facility shall accommodate limits on . . . the time of operation” of a monitoring device.<sup>107</sup>

The temporal dimension of camera use may also be constrained in terms of its *duration* over longer periods of time. In Washington, residents and nursing home facilities must agree in writing “upon a specific duration for the electronic monitoring” to occur.<sup>108</sup> These agreements must be re-evaluated at least quarterly to determine if there is still a “need for” such monitoring.<sup>109</sup>

### F. Situational Constraints

Residents’ rooms are sites in which residents engage in all sorts of intimate activities and interactions, many of which they might not wish to be recorded. In light of this consideration, some states’ rules account specifically for *situations* in which monitoring should—or should not—occur. In our dataset, this occurred both through explicit requirements that a situation present an affirmative case *for* monitoring, and through proscriptions *against* monitoring for specific circumstances and exchanges. In addition, statutory provisions requiring states to protect the

---

105. See *infra* Part V.B. (resident-roommate dyad).

106. 210 ILL. COMP. STAT. 32/15(b) (2017); N.M. STAT. ANN. § 24-26-3(B) (West 2017); UTAH CODE ANN. § 26-21-303(1)(b) (West 2016).

107. N.M. STAT. ANN. § 24-26-3(B) (West 2017). Utah’s provision has similar effect. UTAH CODE ANN. § 26-21-303(1)(b) (West 2016) (conditioning roommates’ consent to monitoring on specific hours of operation). Illinois’s statute does not require that hours of operation be set forth in advance, but provides that residents or roommates can “request that the electronic monitoring device be turned off . . . at any time.” 210 ILL. COMP. STAT. 32/15(b) (2017).

108. WASH. ADMIN. CODE § 388-97-0400(2)(d) (2017).

109. *Id.* at (3)(a).

dignity and privacy of nursing home residents *generally* can be read as a potential constraint on how monitoring is to occur.

As we have described, most of the states in our dataset allow residents (or their legal representatives) to monitor their rooms for any, or no, reason—provided that they pay the costs of monitoring, acquire consent from roommates, and fulfill other institutional requirements.<sup>110</sup> Washington, by contrast, requires residents wishing to operate a monitoring device to provide *affirmative justification* for doing so: a resident must have “identified a threat to the resident’s health, safety or personal property” prior to any monitoring occurring.<sup>111</sup> Washington is the only state in our dataset to take such an approach. This language seems to suggest that monitoring is to be considered as a *defensive* strategy to a foreseen threat, rather than a generalized prophylactic against indiscriminate risk.

Other states do not require affirmative situational justification for monitoring. Instead, some require that monitoring *not occur in particular situational circumstances*, seemingly in recognition of the variety of intimate activities that take place in resident rooms. As we discuss in more detail *infra*, these constraints include residents’ and roommates’ rights of refusal to be monitored under specific circumstances, including visits by specified visitors and service providers.<sup>112</sup>

Finally, statutes in most states in our dataset seek to enshrine nursing home residents’ rights to *dignity*, autonomy, privacy, and similar human and civil rights. Though states’ commitments to these values are not specific to camera use—more commonly, they are reflected in broader purpose-related statutory clauses describing the goals of nursing home governance generally—they can be understood as general values for which nursing homes ought to account in all aspects of their operation, including monitoring schemes. These values are described in varying terms, including that residents be treated with dignity<sup>113</sup> and respect,<sup>114</sup> that their “individuality, privacy, independence, autonomy, and decision-making ability [are promoted],”<sup>115</sup> that they are soundly protected from “physical harm” and “mental anguish,”<sup>116</sup>

---

110. See *supra* Part IV.A.

111. WASH. ADMIN. CODE § 388-97-0400(2)(b) (2017).

112. See *infra* Parts V.B and V.D (roommates and visitors).

113. 210 ILL. COMP. STAT. 9/5 (2017); LA. STAT. ANN. § 2010.8(A)(9) (2018).

114. N.M. STAT. ANN. § 24-17A-4(A) (West 2017).

115. 210 ILL. COMP. STAT. 9/5 (2017).

116. WASH. ADMIN. CODE § 388-97-0001 (2017).

and that they “have privacy in treatment and in caring for personal needs[.]”<sup>117</sup>

### G. Litigation Constraints

The recordings made in resident rooms seem a likely source of probative evidence if they do, in fact, capture indicia of abuse, neglect, or other illegal activities. In addition, the act of recording itself may increase the risk of litigation related to the invasion of residents’ (and potentially others’) privacy. Hence, most states in our dataset took measures in anticipation of the role that recordings might play in lawsuits. These measures are of three general types: measures concerning the *admissibility and authentication* of resident room recordings as evidence, measures *limiting liability* for monitoring-related invasions of privacy, and measures establishing *abuse reporting* rules related to in-room recordings.

Five of the seven states in our dataset established rules governing the *admissibility* of in-room video and audio recordings in civil, criminal, and administrative proceedings. All five established that such recordings *could* be admitted into evidence in such proceedings;<sup>118</sup> four established further conditions for admissibility.<sup>119</sup> Related restrictions concern the *authentication* of recordings. Texas and Illinois require that video recordings be time- and date-stamped, unedited, and not artificially enhanced.<sup>120</sup> Texas further requires that if a recording has been reformatted, “the transfer was done by a qualified professional and the

---

117. LA. STAT. ANN. § 40:2010.8(A)(8) (2018).

118. 210 ILL. COMP. STAT. 32/50 (2017); LA. STAT. ANN. § 40:1193.7(A) (2018); OKLA. STAT. ANN. tit. 63, § 1-1953.4 (West 2017); N.M. STAT. ANN. § 24-26-7(A) (West 2017); TEX. HEALTH & SAFETY CODE ANN. § 242.849(a)-(b) (West 2017).

119. 210 ILL. COMP. STAT. 32/50 (2017) (conditioning admissibility on date/timestamp and lack of editing/artificial enhancement of recording); LA. STAT. ANN. § 40:1193.7(A) (2018), N.M. STAT. ANN. § 24-17A-4(A) (West 2017) (both conditioning admissibility on facility’s knowledge of the monitoring device and required forms having been filled out); TEX. HEALTH & SAFETY CODE ANN. § 242.849(a)-(b) (West 2017) (conditioning admissibility on date/timestamp, lack of editing/artificial enhancement of recording, and any format transfer being done by a “qualified professional,” and other conditions). Oklahoma’s statute establishes that “[s]ubject to the provisions of law,” a recording made under the act “may be admitted into evidence in a civil or criminal court action or administrative proceeding[.]” but establishes no other specific conditions thereon. OKLA. STAT. ANN. tit. 63, § 1-1953.4 (West 2017).

120. TEX. HEALTH & SAFETY CODE ANN. § 242.849(b)(1)-(2) (West 2017); 210 ILL. COMP. STAT. 32/50 (2017). Louisiana also requires visual recordings to be date- and time-stamped. LA. STAT. ANN. § 40:1193.3(A)(2) (2018).

contents of the tape or recording were not altered.”<sup>121</sup> Illinois requires that a resident must tender copies of a relevant recording to parties in a proceeding upon request.<sup>122</sup>

Some states in our dataset (Illinois,<sup>123</sup> New Mexico,<sup>124</sup> Utah,<sup>125</sup> Texas,<sup>126</sup> and Louisiana)<sup>127</sup> *limit liability* for nursing homes for violations of residents’ privacy that arise from electronic monitoring. Two states address the liability of residents themselves for claims regarding monitoring.<sup>128</sup>

Interestingly, two states in our dataset—Texas and Louisiana—establish rules regarding the role of recordings from in-room monitors in *abuse reporting* processes. Texas has established a statutory duty for nursing home owners and employees to report abuse or neglect to the state’s Department of Family and Protective Services.<sup>129</sup> Its statutes establish that a person conducting electronic monitoring on behalf of a resident “is considered to have viewed or listened to . . . a recording made by the electronic monitoring device” within fourteen days of the recording being made, for purposes of reporting any evidence of abuse or neglect to the state.<sup>130</sup> The person is required to report abuse if “the incident of abuse is acquired” on the recording or if “it is clear from viewing or listening to [it] that neglect has occurred.”<sup>131</sup> Louisiana’s law

121. TEX. HEALTH & SAFETY CODE ANN. § 242.849(b)(3) (West 2017).

122. 210 ILL. COMP. STAT. 32/45 (2017).

123. 210 ILL. COMP. STAT. 32/60(b) (2017).

124. N.M. STAT. ANN. § 24-26-5(B) (West 2017).

125. UTAH CODE ANN. § 26-21-303(2) (West 2016).

126. TEX. HEALTH & SAFETY CODE ANN. § 242.846(b)(1) (West 2017) (for residents conducting monitoring); TEX. HEALTH & SAFETY CODE ANN. § 242.846(d) (West 2017) (for roommates in monitored rooms).

127. LA. STAT. ANN. § 40:1193.5(B) (2018).

128. Compliance with the New Mexico monitoring statute is deemed a “complete defense” against civil and criminal actions brought against the facility or residents and surrogates for use of a monitoring device. N.M. STAT. ANN. § 24-26-7(B) (West 2017). In Texas, by contrast, nursing home residents are required to sign a form recognizing that they may be civilly liable for violating privacy rights if they use a monitoring device or disclose a recording. TEX. HEALTH & SAFETY CODE ANN. § 242.844(1) (West 2017).

129. TEX. HEALTH & SAFETY CODE ANN. § 260A.002 (West 2017).

130. TEX. HEALTH & SAFETY CODE ANN. § 242.848(a) (West 2017). Time constraints also apply if a resident conducting monitoring gives a recording to someone else to view or listen to it. TEX. HEALTH & SAFETY CODE ANN. § 242.848(b) (West 2017) (establishing a seven-day window for reporting abuse or neglect after receiving such a recording).

131. TEX. HEALTH & SAFETY CODE ANN. § 242.848(c) (West 2017). The statute also contains a measure that requires a person sending multiple recordings to the

similarly requires reporting from “[a]ny person who views an incident which a reasonable man would consider abuse or neglect” to the nursing facility.<sup>132</sup> These provisions provide recognition of the potential evidentiary value of recordings in the reporting and adjudication of abuse complaints—and hedge against recorded evidence being lost to state bureaucracy by shifting the burden of abuse remediation from the nursing home resident to the facility upon production of such recordings.

\* \* \*

These seven forms of constraint demonstrate multiple approaches to privacy protection with respect to in-room camera use. These approaches range from familiar notice-and-consent frameworks to mandates regarding what types of data can be captured, and in what situations. Based on this taxonomy, we seek next to evaluate how such forms of constraint protect and balance the interests of various stakeholders in the nursing home setting, and to consider what such an analysis reveals about how privacy within complex relational contexts is conceived.

## V. For and Against Whom is Privacy Protected? Mapping Privacy Relations

This section turns specifically to the relational dimensions of privacy protection in the nursing home context. We began our analysis by creating a network map and listing a comprehensive set of relational dyads among five key stakeholders in the nursing home context. The identified stakeholders include residents, residents’ family representatives, roommates, nursing home employees, and nursing home facilities as state actors. Once we created this list, we considered each relationship through the lens of our taxonomy of privacy constraints (discussed in Part IV), including attention to statutory and regulatory provisions that evinced specific applicability to particular relationships. This examination sought to determine how effectively the constraints address privacy and security concerns present in different dyads. Specifically, we assessed when and how various constraints seemed geared toward perceived threats arising within a particular relationship, and how they aimed to protect one party to the relationship

---

state to pinpoint ostensible evidence of abuse or neglect—presumably to reduce administrative burdens of combing through hours of recordings. TEX. HEALTH & SAFETY CODE ANN. § 242.849(c) (West 2017).

132. LA. STAT. ANN. § 40:1193.10 (2018).

vis-à-vis the other. In so doing, we elucidated common and uncommon regulatory strengths and seeming limitations.

Given the impracticality of presenting analysis of all dyads, we selected five relationships of primary interest, which are described below.

#### A. Relations Between Residents and Family Representatives

As discussed in Part II, roughly half of nursing home residents have Alzheimer's disease or related dementias. As such, many residents' personal interests are represented by other parties who serve as their legal representatives or surrogates—commonly, family members.<sup>133</sup>

Residents with advanced dementias may require more protection against abuse, neglect, or theft because they are perceived as especially vulnerable targets, and are unable to reliably report mistreatment. Concomitantly, these residents often lack the capacity to make decisions about in-room camera use—most notably, the capacity to consent to such monitoring, and to condition such consent upon various constraints (temporal, situational, and the like). But a resident's reduced capacity may *increase* family members' desire to install monitoring equipment, based on a perceived need to protect them from mistreatment at the hands of others (for instance, nursing home workers).

States account for the resident-representative relationship by explicitly denoting that family representatives may be the primary decision-makers regarding camera use. The majority of the laws we analyzed contain language clarifying that a resident *or her representative* can consent to monitoring and place limitations thereon.<sup>134</sup> These provisions provide legal recognition of one common aspect of the resident-representative relationship: the representative may be the *primary advocate* of the resident's privacy and security interests against perceived external threats to each.

---

133. See G.D. Rowles & D.M. High, *Individualized Care: Family Roles in Nursing Home Decision-Making*, 22 J. OF GERONTOLOGICAL NURSING 20 (1996); see also D.M. High & G.D. Rowles, *Nursing Home Residents, Families, and Decision Making: Toward an Understanding of Progressive Surrogacy*, 9 J. AGING STUD. 101, 103 (1995).

134. See, e.g., Oklahoma (OKLA. STAT. ANN. tit. 63, § 1-1953.5 (A) (West 2017)), Utah (UTAH CODE ANN. § 26-21-303(1) (West 2016)).

However, this privacy decision-making capacity is not without risks. As we have described,<sup>135</sup> residents who lack decision-making capacity may not be consulted at all about monitoring in their rooms—which means that legal representatives risk making decisions to which the resident would not have agreed. Most of the laws we analyzed do not account for potentially inconsistent privacy preferences between a resident and her representative; generally, they envision representatives' interests as an exact extension of residents' interests, and offer no provisions that structure how representatives formulate their monitoring plans. This latitude can create the conditions for representatives to monitor residents with reduced capacities in ways they would not have agreed to if they were lucid.

Even more fundamentally, monitoring provisions generally do not account for potential abuse situations *within* the resident-representative relation. Because representatives are most commonly family members, this relationship is complicated by the myriad relational dynamics inherent in families. Recent scholarship suggests that adult children and spouses—parties very likely to serve as residents' representatives—are the most common perpetrators of elder abuse.<sup>136</sup> Clearly, if the representative is herself mistreating the resident, cameras are likely to be an ineffective preventative measure against such abuse—either because the representative is unlikely to install a camera in the first place, or because if a camera is in use, she likely controls the captured data.

Washington provides one counterexample: the state conditions the rigor of consent requirements on the type of monitoring to be used. In Washington, a resident's representative may consent on her behalf to video monitoring *without* an audio component—but only a “court-appointed guardian or attorney-in-fact” may consent on the resident's behalf to *audio* monitoring, and must “obtain[] a court order specifically authorizing” him or her to do so.<sup>137</sup> This provision signals that some lawmakers are aware that residents may not always completely entrust privacy decision-making to their representatives, and use a technological constraint (a restriction on the type of data to be captured) to effect privacy protection.

---

135. See discussion of survey responses in Part II; see also *Cameras on Beds*, *supra* note 19.

136. Lachs, *supra* note 23.

137. WASH. ADMIN. CODE § 388-97-0400(5)-(6) (2017).

Illinois takes a different approach, articulating a more detailed consent process that takes likelihood of limited capacity and inconsistent preferences into account. Illinois only permits representatives to consent to monitoring on a resident's behalf *if* "the resident *has not affirmatively objected* to the authorized electronic monitoring, and the resident's physician determines that the resident *lacks the ability to understand and appreciate the nature and consequences* of electronic monitoring."<sup>138</sup> Should these conditions be met, Illinois requires that the resident *must be asked* by the representative, *in the presence of a facility employee*, if she wants authorized electronic monitoring to be conducted in her room—and that the representative must explain to the resident what sort of device will be used, with whom the recording can be shared, what conditions may be placed on the device's use, and the resident's ability to decline recording altogether.<sup>139</sup> The statute *further* notes that a resident is deemed to object "when he or she orally, visually, or through the use of auxiliary aids or services declines authorized electronic monitoring."<sup>140</sup> By far, Illinois's statute mandates the most detailed procedure governing the resident-representative relationship, and seems to anticipate the potential for representatives to disrespect residents' privacy preferences (e.g., by requiring a facility employee to be present when the resident is asked about monitoring, and by delineating what sorts of communications constitute objections that a representative may not override).

Even short of abuse or willful disrespect of residents' preferences, monitoring may readily engender privacy violations within the resident-representative relationship due to the intimacy of the activities that take place in resident rooms. A resident's privacy may be violated *by her representative* if her family member has access to a video or audio feed of her every interaction and behavior within her room. In addition, representatives' exclusive access to recordings can create opportunities to intimidate or extort a resident with embarrassing footage. State laws—with the notable exception of the Washington and Illinois provisions—do little to protect against such violations.

States' hands-off approaches to privacy and security risks between family members is an interesting reflection of the broader ethos

---

138. 210 ILL. COMP. STAT. 32/15(a) (2017) (emphasis added).

139. 210 ILL. COMP. STAT. 32/15(a-5) (2017) (emphasis added).

140. *Id.*

underlying camera laws. While camera laws effectively reflect the extension of responsibility to families for care and protection of their elderly relatives—even in state-funded residences—the converse appears not to hold: families are obliged to protect against mistreatment by nursing homes using cameras, but states effectively stay out of families' business by not taking steps to protect residents against privacy invasions from family members.

In sum, these laws evince the tacit presumption that residents' and their representatives' privacy interests are always in lockstep. In reality, cameras are a double-edged surveillance tool: while laws that give family members decision-making authority can help protect residents with diminished capacity against external threats, they may increase the risk of privacy invasions within family relations.<sup>141</sup>

## B. Relations Between Residents and Roommates

Nursing homes represent a hybrid of shared and private space, as many resident rooms accommodate two occupants living separately but together as roommates. A chief area of concern is negotiating how one occupant's desire to use a monitoring device can be honored, while also respecting another occupant's desire to be unmonitored, or monitored in very limited ways. Achieving an agreeable balance between these two sets of interests can substantially complicate implementation of monitoring regimes.

Unlike the resident-representative relationship, the laws we considered do take explicit account of potentially incompatible preferences between residents and their roommates, and employ many forms of privacy constraint to balance between them. All states we analyzed require written consent from roommates or their representatives<sup>142</sup> before monitoring in their room can occur (a *bureaucratic* constraint).<sup>143</sup>

---

141. Tracy Kohl, Comment, *Watching Out for Grandma: Video Cameras in Nursing Homes May Help Eliminate Abuse*, 30 FORDHAM URB. L. J. 2038, 2097 (2003) (acknowledging that roommates have a privacy interest at stake as well).

142. Of course, roommates and their representatives may have inconsistent privacy preferences, just as monitoring residents and their representatives do. See *supra* Part V.A. The limitations brought about by those potential inconsistencies are unaddressed in the law, and further complicate the resident/roommate relationship; in practice, monitoring may be negotiated between representatives of both resident and roommate, rather than the parties themselves.

143. See *supra* Part IV.A.

*Spatial* constraints, as described in Part IV.D., are another principal tool for protecting roommates' privacy. For example, in Texas, a roommate can condition her consent to monitoring on the camera being "pointed away" from her.<sup>144</sup> In addition, several provisions enable residents to change rooms (and require reasonable accommodations for doing so from nursing homes) should a resident's monitoring preferences be wholly incompatible with the wishes of roommates.<sup>145</sup>

*Temporal* constraints give a roommate the ability to restrict her consent to monitoring to specific hours when the camera is allowed to operate and record data. For example, in Utah, a resident wishing to monitor a shared room must obtain written consent from her roommates (or their legal representatives) "that specifically states the hours when each roommate consents"<sup>146</sup> to operation of the monitoring device. *Technological* constraints may also be employed, such as Illinois's and Texas's provisions allowing roommates to condition electronic monitoring on the prohibition of audio data collection.<sup>147</sup>

By contemplating such constraints and permitting roommates to condition monitoring thereon, states demonstrate a sensitivity to the needs of balancing incompatible privacy preferences in shared spaces. Moreover, these considerations illustrate a recognition of the interdependent nature of privacy relations: a monitoring relationship between, for example, a resident and her family member has certain impacts on third parties, even if those parties are not primary targets of monitoring.<sup>148</sup>

In some cases, a roommate may herself be a perceived abuse threat.<sup>149</sup> Texas is the only state we analyzed that permits *covert* monitoring, which strikes a different balance between residents' and roommates' interests. To conduct "authorized" monitoring in Texas, as in other states, a resident (or her representative) must obtain roommate consent.<sup>150</sup> However, Texas's law alternatively provides for "covert" monitoring, in which the resident or representative monitors a room in

---

144. TEX. HEALTH & SAFETY CODE ANN. § 242.846(e)(1) (West 2017).

145. See e.g., 210 ILL. COMP. STAT. 32/15(e) (2017).

146. UTAH CODE ANN. § 26-21-303(1)(b) (West 2016) (setting forth requirements of written consent, which includes the hours roommate(s) consent to video recording).

147. 210 ILL. COMP. STAT. 32/20(B)(7)(a) (2017); TEX. HEALTH & SAFETY CODE ANN. § 242.846(e)(2)(B) (West 2017).

148. See Levy & Barocas, *supra* note 16, at 1.

149. See Gibbs & Mosqueda, *supra* note 23, at 32.

150. TEX. HEALTH & SAFETY CODE ANN. § 242.846(b)(3) (West 2017).

a way that is not open and obvious, and without informing the nursing home that she is doing so.<sup>151</sup> Under covert monitoring, no mention is made of a need to obtain roommate consent (and such a requirement would clearly be difficult for the facility to enforce).<sup>152</sup> Though the state limits its own liability for harms arising from covert monitoring, it offers some protection to residents who engage in it: Texas law prevents nursing homes from removing residents who covertly monitor their rooms.<sup>153</sup> Covert monitoring thus prioritizes a resident's interests over those of an unaware and potentially nonconsenting roommate.

In practice, provisions to protect roommates' privacy interests may be difficult to implement pragmatically. For example, depending on the design of the shared quarters, it is unclear to what degree it is possible to point a camera away from a roommate to honor their privacy preferences. Similarly, provisions allowing nonconsenting roommates to move to a new (unmonitored) room presume that a more suitable space is available. Further, many of these constraints rely heavily on frequent human action to ensure compliance (e.g., to point a camera away from one part of a room, to turn a camera off during certain hours of the day, etc.). States are nonspecific about who is responsible for ensuring that conditions are met (e.g., the resident conducting the monitoring, a facility employee, etc.), and who is accountable if they are not. Reliance on human action to ensure roommate privacy creates the conditions for them to be accidentally or purposively neglected. Nursing homes are busy, understaffed, and under-resourced spaces.<sup>154</sup> Workers

---

151. TEX. HEALTH & SAFETY CODE ANN. § 242.843(a) (West 2017). Texas limits its liability for harms related to covert monitoring. *See infra* Part V.E.

152. Nursing home residents in Texas fill out a form upon admission that may inform them *generally* about the potential use of covert and authorized monitoring in resident rooms, but no notification of covert monitoring in their *own* room. TEX. HEALTH & SAFETY CODE ANN. § 242.844 (West 2017). Further, if a facility discovers covert monitoring, the person conducting the monitoring will be required to meet the requirements for authorized monitoring, which include roommate consent. 40 TEX. ADMIN. CODE § 19.422 (2017).

153. TEX. HEALTH & SAFETY CODE ANN. § 242.847(a) (West 2017).

154. *See* Clara Berridge et al., *Staff Empowerment Practices and CNA Retention: Findings From a Nationally Representative Nursing Home Culture Change Survey*, 37 J. APPLIED GERONTOLOGY 419, 421 (2016) [hereinafter *Staff Empowerment Practices*]; D. Shipman & J. Hooten, *Are Nursing Homes Adequately Staffed? The Silent Epidemic of Malnutrition and Dehydration in Nursing Homes Residents*, 33 J. GERONTOLOGICAL NURSING 15 (2007); L. Harris et al., *Recent Findings on Frontline Long-Term Care Workers: A Research Synthesis 1999-2003*, INST. FOR FUTURE AGING SERVICES (May 2004), <http://www.aspe.hhs.gov/system/files/pdf/73241/insight.pdf> (Section VII); Nat'l Citizens' Coal. for Nursing Home Reform, *The Nurse Staffing Crisis in Nursing*

are severely overburdened with job duties and must perform them quickly,<sup>155</sup> making it unlikely that they will be able to prioritize tasks like turning cameras on and off each day. The residents and roommates who lack capacity are unlikely to be able to enforce these constraints themselves or to request that workers do so. Hence, given the social realities of the context, constraints to protect roommates' privacy may be practically ineffective.

### C. Relations Between Residents and Nursing Home Employees

As described in Part II, a primary driver of in-room camera use is concern about abuse at the hands of nursing home staff; placing a camera in a resident's room is intended to capture evidence of or deter such abuse.<sup>156</sup> As discussed, the perceived threat of abuse by nursing home employees may be outsized in the public imagination relative to threats of abuse by other parties (other nursing home residents, family members). However, the deployment of cameras into resident rooms can also be viewed through the lens of increasing surveillance in low-wage workplaces,<sup>157</sup> as well as increased surveillance of care work.<sup>158</sup> The nursing home is, after all, a workplace—and one which predominantly employs women of color, for relatively low pay. In addition, nursing home workers are generally not unionized, and lack much power over workplace conditions.<sup>159</sup>

---

*Homes Consensus Statement of the Campaign for Quality Care*, THE NAT'L CONSUMER VOICE FOR QUALITY LONG-TERM CARE 3 (June 26, 2001), [http://theconsumerveice.org/uploads/files/issues/Consensus\\_Statement\\_Staffing.pdf](http://theconsumerveice.org/uploads/files/issues/Consensus_Statement_Staffing.pdf); Robyn I. Stone and Joshua M. Wiener, *Who Will Care For Us? Addressing the Long-Term Care Workforce Crisis*, THE URB. INST. (2001), [http://www.forschungsnetzwerk.at/downloadpub/2001\\_Who\\_will\\_Care\\_for\\_Us.pdf](http://www.forschungsnetzwerk.at/downloadpub/2001_Who_will_Care_for_Us.pdf).

155. See *supra* Part II; see generally Acierno et al., *supra* note 24.

156. See *supra* note Part II.

157. See generally Karen E.C. Levy, *The Context of Control: Information, Power, and Truck-Driving Work*, 31 INFO. SOC'Y 160 (2015) (examining the implications of electronic monitoring systems in the trucking industry); Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U. L. REV. 53, 60 (2017) (discussing use of surveillance in low-wage workplaces).

158. See, e.g., Stark & Levy, *supra* note 8 (describing consumer-driven surveillance of care workers such as nannies); Karin Willison, *Federal Law Now Requires States to GPS Track Disabled People Who Use Attendants*, THE MIGHTY (January 19, 2018), <https://themighty.com/2018/01/electronic-visit-verification-gps-tracking-disabled-people/>.

159. See *Staff Empowerment Practices*, *supra* note 154, at 421; Clara Berridge et al., *Staffing Empowerment Practices in Nursing Homes with Unionized Nursing Assistants*, 1 INNOVATION IN AGING 286 (2017).

State laws predominantly protect worker privacy through *visual* constraints—specifically, signage requirements that provide notice of monitoring within a room.<sup>160</sup> Notice of surveillance can be understood as a sort of privacy protection, in that workers can modulate their behavior in spaces they know to be monitored. Notice of surveillance can certainly function as a deterrent to threats of abuse promulgated by workers, by suggesting that maltreatment will be made visible; however, it may also chill other non-abusive behaviors in the workplace (e.g., sensitive conversations with residents).

Theoretically, making people aware that monitoring is underway deputizes them to *protect their own privacy* through enabling them to avoid or remove themselves from locations and situations where monitoring is occurring. However, unlike other people who might enter a monitored room—like a family member or social visitor—staff often *do not have the choice to enter a room or not*, as working in monitored space is required to provide care for residents. There were no indications that the legal regimes we analyzed provided any processes for obtaining consent from workers; rather, as in other workplaces, consent is considered to be implied by continued employment. The absence of privacy protections specific to workers surfaces underlying presumptions that workers are predominantly parties *against whom* monitoring is deployed, rather than parties whose own privacy interests are at stake.

#### D. Relations Between Residents and Visitors

Some residents receive frequent visitors in their rooms: family, friends, religious advisors, health care professionals, attorneys, and numerous others. The circulation of visitors into monitored resident rooms can undermine the privacy of their interactions with residents, which may be quite sensitive in nature. Because visitors are likely to be only occasionally present within resident rooms, they may have less familiarity with monitoring regimes than other parties (workers, roommates, or residents)—and have less ability to consent to or place conditions upon being monitored while in the room. In addition, residents may *themselves* desire extra privacy when visitors are present to discuss sensitive matters.<sup>161</sup>

---

160. See Calo, *supra* note 21, at 1030.

161. Of course, visitors may also be perpetrators of abuse against residents—in which case it is in residents' interests that their interactions be captured.

*Situational* constraints in some legal regimes demonstrate recognition of these interests. Some specifications acknowledge the private nature of specific social *exchanges and practices*, rather than protecting privacy through controls on particular data types, institutional restrictions, or other means.<sup>162</sup> For example, Illinois's statute specifies that nursing homes' consent forms for electronic monitoring contain:

[A] list of standard conditions or restrictions that the resident or a roommate may elect to place on use of the electronic monitoring device, including, but not limited to [. . .] turning off the electronic monitoring device or blocking [its] visual recording component [. . .] for the duration of an exam or procedure by a health care professional[, . . .] while dressing or bathing is performed[, and . . .] for the duration of a visit with a spiritual advisor, ombudsman, attorney, financial planner, intimate partner, or other visitor[.]<sup>163</sup>

Similarly, in Texas, the roommate of a resident who wishes to install monitoring equipment must fill out a form indicating "whether the camera should be obstructed in specified circumstances to protect the dignity" of the roommate;<sup>164</sup> the statute does not delineate what these circumstances might be. Though the consenting party under the Illinois and Texas statutes is still the resident or roommate—rather than the visitor herself—this provision acknowledges that some situations, including visits, may occasion additional privacy protections.

In other regimes, *visual* constraints provide some protections for visitors' privacy. As with nursing home workers, signage outside rooms can serve as notification of monitoring to visitors.<sup>165</sup> In addition, some states require that signs be posted at entrances to the *facility*, notifying those who enter that monitoring devices are being used within residents' rooms. Illinois states that such signs must be placed at "all building entrances accessible to *visitors*,"<sup>166</sup> and Oklahoma states that such signs must be placed "at or near its main entrances."<sup>167</sup> These pro-

---

162. See generally NISSENBAUM, *supra* note 13 (describing privacy as dependent on appropriate norms of information flow within a given social context).

163. 210 ILL. COMP. STAT. 32/20(b)(7)(C)-(E) (2017) (emphasis added).

164. TEX. HEALTH & SAFETY CODE ANN. § 242.846(b)(2) (West 2017). See also 40 TEX. ADMIN. CODE § 19.422(f)(3) (West 2017) ("The [nursing home] facility must meet residents' requests to have a video camera obstructed to protect their dignity.").

165. See *supra* Part V.C.

166. 210 ILL. COMP. STAT. 32/30(a) (2017) (emphasis added).

167. OKLA. STAT. ANN. tit. 63, § 1-1953.2(C) (West 2017).

visions specifically target the interests of occasional visitors by providing more global notice of monitoring at points where visitors are likely to encounter them.

These safeguards do not perfectly ensure that visitors' privacy interests are protected. As we have discussed, required visual notice effectively charges people with the responsibility to protect their own privacy by making them aware that monitoring is occurring – but does not give them the right to withhold consent from being monitored, except by not entering the space.<sup>168</sup> Different types of visitors may have more or less autonomy to decide whether to visit a resident room or not (we might imagine, for instance, that friends have more autonomy to do so, while health care professionals have less). Similarly, because consent to situational constraints depends on residents and roommates – not visitors – the degree to which visitors are monitored is at the discretion of how much the monitoring resident or roommate wishes to be recorded on camera *with them*. In this way, room residents are the arbiters of the degree to which visitors experience privacy when in their rooms.

#### **E. Relations Between Residents and the State**

Recordings made in resident rooms may serve as evidence of abuse or neglect in civil actions against the state. Nursing home facilities, of course, have a strong interest in avoiding liability for the abuse of their residents. To this end, states tend to protect their own interests through *litigation* constraints, such as restrictions on admissibility and requirements for authentication of recordings. One interesting approach conditions admissibility upon *bureaucratic* constraints: New Mexico, for example, bars the use of material from in-room monitors in civil actions against the facility “if the monitoring device was installed or used without the knowledge of the facility or without the prescribed form.”<sup>169</sup> This technique frames bureaucratic constraints as a form of notice to the facility itself about the presence of a monitoring device.

In addition, the act of recording itself may pose litigation risks related to the invasion of residents' (and potentially others') privacy. Litigation constraints are commonly used here as well. As described in Part IV.G, most of the regimes we analyzed explicitly limited nursing

---

168. See generally Jones, *supra* note 7 (describing limitations of privacy protections for incidental guests in spaces like smart homes).

169. N.M. STAT. ANN. § 24-26-7(A) (West 2017).

homes' liability for violations of residents' privacy arising from camera use. In Utah, residents and residents' roommates waive civil and criminal claims against facilities for the operation of monitoring devices; facilities are also not liable to "any person *other* than the resident or resident's roommate for *any* claims related to the use and operation of a monitoring device [. . .] unless the claim is caused by the acts or omissions of an employee or agent of the facility."<sup>170</sup> Illinois limits nursing homes' liability for "inadvertent or intentional disclosure of a recording" by a resident or her representative.<sup>171</sup> In Texas, a nursing home may not be held civilly liable for the use of electronic monitoring if that placement is "covert"<sup>172</sup>—and residents who covertly monitor a room waive privacy rights they have "in connection with images or sounds that may be acquired by the device."<sup>173</sup>

*Bureaucratic* constraints also have a role here. By formalizing the procedures residents must go through in order to use cameras, and by requiring signed consent forms from residents, representatives, and roommates, states create documentary records from likely litigants that can presumably be used to undercut privacy tort claims against them. In addition, *technological* constraints—particularly limits on what sorts of data may be captured, as well as rules about encryption and network connectedness—regulate access to and security of data by governing the circumstances under which monitoring records can be accessed and viewed.

The majority of these constraints serve to insulate states from the potentially costly claims that may arise from, or be bolstered by, monitoring. In a sense, these measures serve as a counterweight to the additional risks states face when residents and their families operate monitoring equipment in state facilities. Yet, as we have described, states have effectively *consumerized* care by offloading much of the responsibility for elder protection to residents and families, through camera measures and a range of other consumer "empowerment" tools—despite the practical difficulties consumers have in effectively making choices in the limited market of available facility options. Subsequent

---

170. UTAH CODE ANN. § 26-21-303(2) (West 2016) (emphasis added).

171. 210 ILL. COMP. STAT. 32/60(a) (2017).

172. TEX. HEALTH & SAFETY CODE ANN. § 242.843(b) (West 2017).

173. TEX. HEALTH & SAFETY CODE ANN. § 242.844(2) (West 2017).

restrictions on the recourse residents can attain *even under such conditions* serves to further undermine the protections available to some of the most vulnerable members of society.

Table 2: How Law Maps Privacy Constraints to Stakeholder Relationships

Relationship	Key privacy concerns	Key constraints	Limitations
Resident/family representative	Resident's limited decision-making capacity	<i>Bureaucratic</i> : permitting representatives to instigate monitoring in cases of limited capacity	Failure to account for abuse, privacy violations, and inconsistent privacy preferences <i>within</i> the relationship
Resident/roommate	Balancing privacy interests in shared space; potential abuse between roommates	<i>Bureaucratic</i> : required notice & consent by roommates (except in cases of covert monitoring)  <i>Spatial</i> : allowing roommates to condition consent on camera scope/place-ment  <i>Temporal</i> : allowing roommates to condition consent on hours of operation  <i>Technological</i> : allowing roommates to condition consent on type of data collected	Constraints rely largely on frequent human action, which may be difficult to implement pragmatically given underresourced context
Resident/nursing home employee	Workers' privacy interests (resident room as workplace)	<i>Visual</i> : signage notifies workers about monitoring	No real consent processes for workers
Resident/visitor	Sensitivity of visits for both residents and visitors	<i>Situational</i> : limitations for given circumstances, values  <i>Visual</i> : signage at visitor entrances	Visitors have limited discretion to withhold consent to monitoring

Resident/state	Limiting liability for abuse and for privacy violations	<p><i>Litigation:</i> rules governing admissibility of recordings, explicit liability waivers</p> <p><i>Bureaucratic:</i> signed consent forms from likely litigants</p> <p><i>Technological:</i> restraints on data access and security</p>	Liability limitations and admissibility rules can restrict recourse available to residents
----------------	---	--	--

## VI. Privacy, Relationships, and the Consumerization of Care

The privacy interests, rights, and dignities of older adults in the digital age are pressing concerns as rapid population aging contributes to unprecedented demand on human and financial care resources.<sup>174</sup> The growing gap between care demand and supply may entrench conditions that promote suboptimal care, abuse, and neglect. The states and nursing home industry have been slow to implement effective, systemic changes in response to these concerns—leaving family members few options when they suspect abuse or poor care. The turn to electronic surveillance, and states' institutionalization of this response through law, accords with broader trends towards consumer responsibility for care, reflected in consumer advocacy and consumer empowerment initiatives that provide information about facility characteristics and records for enhanced private decision-making. Like these consumer responsibility approaches, we find that state electronic monitoring laws have notable limitations, particularly when we consider the privacy interests of the most vulnerable stakeholders: residents and workers.

By examining how privacy interests are treated and prioritized in these state laws, we find an unresolved need to ensure that residents'

174. See Barbara Cire, *World's Older Population Grows Dramatically: NIH-Funded Census Bureau Report Offers Details of Global Aging Phenomenon*, NAT'L INST. ON AGING (Mar. 28, 2016), <https://www.nih.gov/news-events/news-releases/worlds-older-population-grows-dramatically>.

priorities are sufficiently represented and their vulnerabilities protected when cameras are used. Laws are particularly limited in the degree to which they address the potential for conflict between residents and their legal representatives regarding decisions about camera use. This reflects states' hands-off approach to family conflict in decision making about camera use, and the risk that family members—the most common perpetrators of elder abuse—will use the information collected by cameras to control or abuse residents. Electronic monitoring in intimate relations thus has a paradoxical potential: it allows monitoring individuals to both protect against and perpetrate abuse. In so doing, it both addresses existing vulnerabilities and creates new vulnerabilities.

The privacy interests of direct care workers are also unaddressed by most monitoring regimes, which conceptualize them as threats, rather than as themselves a vulnerable group. This treatment could have a deterring effect for would-be career nursing assistants, whose work is already characterized by low-value assignment of wages, benefits, and respect.<sup>175</sup> In this context of poorly remunerated and socially devalued work, rewards such as negotiating and enjoying trusting relationships, positive recognition, and dignity in the labor of sustaining and enriching residents' lives may be critical to workforce attraction and retention. The assumption that nursing assistants will work on camera without being involved as stakeholders in these decisions has not been tested. Considering the positionality of both residents and workers, we raise the question of how surveilled resident rooms will affect the quality of care relationships, as well as job quality for this high-demand workforce.

As lightweight, consumer-grade surveillance devices continue to infiltrate shared spaces, and as we continue to manage our most intimate relationships using these tools, social roles and privacy interests blur and mix in complex configurations. The nursing home context offers an instructive case that can inform our thinking about privacy regulation more broadly. The seven legal regimes we analyzed evidence a broad range of approaches through which law contends with conflicting privacy and security concerns among diverse stakeholders. The regimes demonstrate a variety of ways of grappling with the unique vulnerabilities faced by different groups, and develop different social,

---

175. See *Cameras on Beds*, *supra* note 19 (in which survey respondents voiced concerns about cameras' chilling and demoralizing effects on nursing home staff).

technical, and institutional levers for balancing multiple privacy goals. They account, to varying degrees, for the relational nature of privacy in the space—by prioritizing safeguards on certain stakeholders’ interests at the expense of others, by positing certain actors as targets and others as threats. In so doing, these laws demonstrate the interdependent nature of privacy in multiplex social spaces, whereby monitoring relations, and constraints thereon, necessarily impact the privacy experiences of others.

