Buffalo Human Rights Law Review

Volume 26 Article 8

1-1-2020

Open Record Laws: Balancing the "Right to Know" with the Safety of Reproductive Health Care Service Providers

Rebecca Bentley
University at Buffalo School of Law (Student)

OPEN RECORD LAWS: BALANCING THE "RIGHT TO KNOW" WITH THE SAFETY OF REPRODUCTIVE HEALTH CARE SERVICE PROVIDERS

Rebecca Bentley†

INTRODUCTION

In 2018, Joseph Jackson was charged with making terroristic threats against a Planned Parenthood in Pittsburgh, Pennsylvania.[1] Enraged that doctors allowed his girlfriend to have an abortion against his wishes, Jackson stated that he found out who the clinicians were who aborted his child and that he knew five houses from which he could steal an AR-15.[2] He posted on Facebook: "I did my research and I found out wh[ich] clinicians aborted my child and I know where they live. . . . You killed the wrong man's child. . . . I wonder if I will get the proper treatment after this. It's time murderers pay for being murderers."[3] In another case, an anti-abortion protestor stalked and threatened a doctor by posting the doctor's name, photo, address, make and model of car, and license plate number on a blog, alongside instructions on how to kill her.[4] The protestor then proceeded to send the doctor's personal information to individuals incarcerated for crimes against abortion providers.[5]

Such on-going threats to the lives and physical safety of reproductive health care service providers is a phenomenon that occurs broadly through-

---

† Rebecca Bentley, J.D. Candidate (B.A., University at Albany) is a member of the Class of 2021 at the University at Buffalo School of Law. She has extensively focused her legal studies in human rights law and received the Professor Virginia Leary Human Rights Fellowship. She would like to thank the *Buffalo Human Rights Law Review* panel for selecting this piece for publication and Professor Tara Melish for her thoughtful suggestions during the editing process.

1. Andrew Goldstein, *'I Know Where They Live.' West Virginia Man Threatens Planned Parenthood Pittsburgh*, PITTSBURGH POST-GAZETTE (Mar. 22, 2018), https://www.post-gazette.com/local/city/2018/03/21/Man-charged-with-threatening-Planned-Parenthood-office-in-Pittsburgh-taylor-swift/stories/201803210263.

2. *Id.*

3. *Id.*

4. Brief for Respondents Delaware County Women's Center et al. at 7, Crocco v. Pa. Dep't of Health, 214 A.3d 316 (Pa. Commw. Ct. 2019).

5. *Id.*

out the United States.[6] Entire websites have indeed been created that are dedicated to posting the names, photographs, spouses' names, and home addresses of reproductive health care service providers, clinics, employees, volunteers, and patients.[7] The National Abortion Federation ("NAF") Violence and Disruption Statistics show that reproductive health care service providers across the United States have been harassed, stalked, assaulted, threatened with deadly force, and murdered.[8] Between 1977 and 2018, NAF reported 10,181 incidents of violence against abortion providers and 561,962 incidents of disruption, such as harassment and obstruction of entrances.[9] Over the same period, NAF reported 11 murders of people involved with providing reproductive health care services, 26 attempted murders, and 290 incidents of assault and battery.[10] The number of actual instances is likely far higher.[11]

---

6. *See, e.g.*, National Abortion Federation, *Anti-Abortion Extremists*, https://prochoice.org/education-and-advocacy/violence/anti-abortion-extremists/ ("For more than 30 years anti-abortion extremists have attempted to use violence against abortion providers to advance their own personal and political agendas. They have injured and murdered health care workers across the country and intimidated and harassed patients who need reproductive health care."); Press Release, Insider NJ, Legislature Expands Address Confidentiality Program to Include Sexual Assault Survivors and Reproductive Health Patients and Workers (June 10, 2019), https://www.insidernj.com/press-release/legislature-expands-address-confidentiality-program-include-sexual-assault-survivors-reproductive-health-patients-workers/ ("Abortion clinics nationwide faced a record number of picketing and trespassing incidents in 2018. Clinics and staff also faced increased rates of obstruction, vandalism, and online hate speech[.]") [hereinafter Insider NJ]; National Abortion Federation, *2018 Violence and Disruption Statistics* (2019), https://prochoice.org/wp-content/uploads/2018-Anti-Abortion-Violence-and-Disruption.pdf [hereinafter NAF 2018 statistics]; CAL. GOV'T CODE § 6215 (West 2003) ("Persons and groups that oppose reproductive rights attempt to stop the provision of legal reproductive health care services by threatening reproductive health care service providers, clinics, employees, volunteers, and patients. The names, photographs, spouses' names, and home addresses of these providers, employees, volunteers, and patients have been posted on Internet Web sites. From one Web site list that includes personal information of reproductive health care service providers, seven persons have been murdered and 14 have been injured. As of August 5, 2002, there are 78 Californians listed on this site. The threat of violence toward reproductive health care service providers and those who assist them has clearly extended beyond the clinic and into the home.").

7. *See, e.g.*, CAL. GOV'T CODE § 6215, *supra*.

8. NAF 2018 statistics, *supra* note 6, at 7-10.

9. *Id.*

10. *Id.*

11. *Id.* at 7.

Anti-abortion extremists have used personal data in an effort to identify, threaten, and victimize reproductive health care service providers.[12] One of the many tactics anti-abortion extremists use to intimidate and victimize reproductive health care service providers is disseminating providers' personal identifying information online and urging others to harm them.[13] In order to proceed with their violent plans, anti-abortion extremists typically seek out providers' personal information through whatever means are available to them, including public record laws.[14] They then use this information in an attempt to reduce abortions through intimidation and violence—using the loss of privacy as a weapon.[15]

This Article argues that current open record laws do not strike the appropriate balance between the core purpose of enabling public access to information necessary for informed, participatory democracy and the equally important value of protecting service providers from threats to their lives and well-being. The Article concludes that, in order to ensure that both interests are provided for in law, states should implement an *exemption* for this discrete category of persons in their current open record laws. This exemption would ultimately prevent states and local agencies from disclosing reproductive health care service providers' personal identifying information to the public given the unique dangers they face to their safety.

The Article proceeds in four parts. Part I discusses state open or public record laws, explaining why they have been developed and how they aim to promote transparency within the government. Part II tracks the growth in legislation and policies, which recognize and protect an individual's right to privacy or— "anonymity"—in society. It shows the strengths and weaknesses of using similar legislation and policies to address the risk of harm reproductive health care service providers face when their personal infor-

---

12. For the purposes of this Article, "reproductive health care service providers" or "providers" will include any owner, operator, contractor, agent, or employee of a reproductive health care service facility, or any person who provides or assists in the provision of reproductive health care services.

13. *See* Brief for Respondents, *supra* note 4, at 5-7.

14. For instance, anti-abortion extremist group Created Equal has used personal information to create and distribute "WANTED-style" flyers and posters displaying the photographs, names, and home addresses of physicians. The group has terrorized doctors at their homes in Ohio, New Mexico, California, and other states. *See* Feminist Majority Foundation, *Walking the Gauntlet: Daily Harassment of Women Patients, Clinics, and Health Care Workers* (2019), https://www.feminist.org/anti-abortion-violence/harassment.html.

15. Charles Ornstein, *Activists Pursue Private Abortion Details Using Public Records Laws*, ProPublica (Aug. 25, 2015), https://www.propublica.org/article/activists-pursue-private-abortion-details-using-public-records-laws.

mation is disclosed through public record laws. Part III recommends that states amend their public records laws to include an explicit blanket exemption of disclosure for reproductive health care service providers because it is the best approach to fit their particular needs. Part IV provides sample text for what a state-level blanket exemption might look like and calls for organizations to produce annual reports and statistics that show the threats of harm providers face. It likewise recommends that agencies adopt internal protocols and trainings to reflect a policy of nondisclosure of providers' personal information.

I. THE PURPOSE OF PUBLIC RECORD LAWS

Every state in the United States has some form of freedom of information law, sometimes referred to as "sunshine laws," "public record laws," or "right-to-know laws," that governs public access to government records. These laws stem from the Freedom of Information Act ("FOIA"),[16] a federal statute originally passed in 1966, which provides a right to request access to federal agency records by any person.[17]

The purpose of FOIA is to reflect "our nation's fundamental commitment to open government," and commitment to accountability and transparency.[18] FOIA conforms with the idea that without public access to government-held information, the public would be deprived of information that is vitally important to evaluate the performance of government agencies and necessary to hold accountable the officials and bureaucrats who conduct the nation's business.[19] The rights of individuals to access public records in order to preserve democratic principles, and oversee their elected officials as they engage in the decision-making process, is considered to "lie at the heart of fair and democratic governance."[20] In 1976, the Govern-

16. The Freedom of Information Act ("FOIA"), 5 U.S.C. § 552 (1966).

17. *Id.*; U.S. Dep't of State, *The Freedom of Information Act*, https://foia.state.gov/learn/foia.aspx.

18. Memorandum from the Attorney General on the Department of Justice FOIA Guidelines 1 (Mar. 19, 2009), https://www.justice.gov/sites/default/files/ag/legacy/2009/06/24/foia-memo-march2009.pdf [hereinafter Memorandum from Attorney General].

19. Martin E. Halstuk, *When Secrecy Trumps Transparency: Why the Open Government Act of 2007 Falls Short*, 16 COMMLAW CONSPECTUS 427, 431 (2008) (citing H.R. REP. No. 104-795, at 6-7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 3448, 3449-50).

20. Christopher P. Gerber et al., *The Right-to-Know Law and Sunshine Act: Balancing Transparency and Confidentiality in Local Government*, BOROUGH NEWS 40, 41 (Dec. 2017), http://sianalaw.com/wp-content/uploads/12.17-Borough-News-RTKL-by-CPG-MGC.pdf.

ment in the Sunshine Act ("GSA") amended FOIA, with a view to further expand transparency in the federal government.[21]

The breadth of FOIA's reach is wide, with the term "record" defined broadly to include reports, e-mails, letters, manuals, photos, films, and sound recordings.[22] Despite this push for transparency, the laws do not require that *all* information be disclosed.[23] It has been recognized that competing rights and values may justify nondisclosure of certain information.[24] FOIA places the burden on the agency to justify its decision to refuse disclosure of requested information on the basis of established exemptions and exclusions.[25] This balancing of competing values was recognized in a 1965 Senate Report which read as follows:

> At the same time that a broad philosophy of 'freedom of information' is enacted into law, *it is necessary to protect certain equally important rights of privacy* with respect to certain information in Government files . . . . It is not necessary to conclude that to protect one of the interests, the other must, of necessity, either be abrogated or substantially subordinated. Success lies in providing a workable formula which *encompasses, balances, and protects all interests*, yet places emphasis on the fullest responsible disclosure.[26]

Due to competing values within a democratic society, the disclosure obligation under FOIA is not absolute.[27] FOIA is designed to exclude categories of information considered private, or imperative to protect other important public interests.[28] Exemptions are therefore recognized to protect "national security, personal privacy, privileged records, and law enforcement interests."[29] Under this categorical approach, federal agencies are required to disclose information requested unless it falls under one of nine enumerated exemptions.[30] These exemptions include: [1] classified in-

---

21. Pub. L. No. 94-409, 90 Stat. 1241 (1976) (5 U.S.C. § 552 (b) (2006)). This GSA ultimately clarified Exemption 3, 5 U.S.C. § 552 (b)(3), and focused on the openness of meetings of multi-member agencies to the public. Administrative Conference of the United States, *Government in the Sunshine Act*, 2014-2 (June 5, 2014), https://www.acus.gov/recommendation/government-sunshine-act#_ftnl.

22. 44 U.S.C. § 3301 (2000).

23. *See* 5 U.S.C. § 552 (b).

24. S. REP. No. 89-813, at 38; *see* 5 U.S.C. § 552 (b).

25. 5 U.S.C. § 552 (a)(4)(B).

26. S. REP. No. 89-813, at 38 (emphasis added).

27. *See* 5 U.S.C. § 552 (b).

28. *Id.*; S. REP. No. 89-813, at 38.

29. Memorandum from Attorney General, *supra* note 18, at 1; 5 U.S.C. § 552 (b).

30. U.S. Dep't of Justice, *What is FOIA?,* https://www.foia.gov/about.html; 5 U.S.C. § 552 (b).

formation for national defense or foreign policy, [2] internal personnel rules and practices, [3] information that is exempt under other laws, [4] trade secrets and confidential business information, [5] inter-agency or intra-agency memoranda or letters that are protected by legal privileges, [6] *personnel and medical files*, [7] law enforcement records or information, [8] information concerning bank supervision, and [9] geological and geophysical information.[31] Congress also provided for three "exclusions,"[32] which protect interests pertaining to *personal privacy*, national security, and law enforcement.[33]

Under FOIA, the provision most applicable to the protection of reproductive health care service providers is Exemption 6, which deals with "personnel and medical files."[34] Exemption 6 permits nondisclosure of "personnel and medical files and similar files" when disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy."[35] Under the statute, "privacy encompass[es] the individual's control of information concerning his or her person."[36] The disclosure of certain information, such as names, titles, or salaries, of federal employees have generally not been considered an invasion of privacy because such information is considered "of such a nature that no expectation of privacy exists."[37] Although generally true, there are instances in which this type of personal identifying information has been withheld.[38] For example, due to recent terrorist attacks, the Department of Defense has regularly withheld personal identifying information about particular employees for whom they believe disclosure would "raise security or privacy concerns."[39] Additionally, on the

---

31. *The Freedom of Information Act*, *supra* note 17 (emphasis added); 5 U.S.C. § 552 (b).

32. An "exemption" is when something is left out from the consequences of a rule, while an "exclusion" refers to something not covered by the rule itself. *Exemption & Exclusion*, BLACK'S LAW DICTIONARY (5th ed. 2016). The two terms are used differently, but their effects appear identical.

33. *The Freedom of Information Act*, *supra* note 17; 5 U.S.C. § 552 (c).

34. 5 U.S.C. § 552 (b)(6); Exemption 7(c), 5 U.S.C. § 552 (b)(7)(c), also pertains to the protection of personal privacy interests, but this only includes information gathered for law enforcement purposes.

35. 5 U.S.C. § 552 (b)(6).

36. U.S. Dep't of Justice v. Reporter Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

37. U.S. Dep't of Justice, *Freedom of Information Act Guide: Exemption 6* (2004), https://www.justice.gov/oip/foia-guide-2004-edition-exemption-6#N_4_ [hereinafter DOJ FOIA Guide].

38. *Id.*

39. *Id.* (citing Memorandum for the Department of Defense FOIA Offices 1-2 (Nov. 9, 2001), https://www.acq.osd.mil/dpap/pdi/pc/docs/Withhold-

state level, entire categories of people have been exempt from disclosing certain personal identifying information in an effort to reduce the risk of harm that subset of people face as a result of their job duties.[40] Thus, the statute appears to take into account the real possibility that certain groups of people may face a greater likelihood of harm from disclosure due to their profession.

In considering whether or not to release the information requested when an exception or exemption is implicated, the Supreme Court has expressed the general rule that the identity of a FOIA requester is not to be taken into account; nor, importantly, is the purpose of the request.[41] Instead, the determination turns on "the nature of the requested document and its relationship to" the basic purpose of FOIA, which is "to open agency action to the light of public scrutiny."[42] When a threat to privacy or security exists, the Department of Justice has noted that the threat must be "real" rather than speculative.[43] Whether a real threat exists is determined on an agency basis through internal protocols and procedure, taking into account precedent and context, and on the basis of reasonable foreseeability.[44]

FOIA and GSA have given rise to state and local laws often referred to as "sunshine laws" or "public record laws," implemented to achieve the purposes of FOIA at state and local levels. These public record laws direct state and local agencies to "publish certain types of information, preserve official records, and make those records available to the public upon request."[45] Similar to the interpretation of FOIA, these laws ultimately presume that all state and local government records are subject to public disclosure, but with various exceptions and exemptions in order to account for competing interests.[46]

---

ing_Info_that_IDs_DoD_Personnel_-_Sept_2005.pdf (finding that certain personnel's names can be withheld, while others must be released due to "the nature of their positions and duties," including public affairs and flag officers)).

40. *See* 65 PA. CONS. STAT. § 67.708 (b)(6)(i)(C) (2009).

41. *Reporter Comm. for Freedom of the Press*, 489 U.S. at 771-72.

42. *Id.* at 772 (citing Dep't of the Air Force v. Rose, 425 U.S. 352, 372 (1976)).

43. DOJ FOIA Guide, *supra* note 37, n.39 (citing *Rose*, 425 U.S. at 380 n.19 ("The legislative history is clear that Exemption 6 was directed at threats to privacy interests more palpable than mere possibilities.")).

44. *See* U.S. Dep't of Justice, *What are FOIA Exemptions?,* https://www.foia.gov/faq.html ("The FOIA authorizes agencies to withhold information when they reasonably foresee that disclosure would harm an interest protected by one of these nine exemptions.").

45. Jenna Weaver, *Sunshine & Public Record Laws: Using Technology To Share Information*, CLEARPOINT STRATEGY: LOC. GOV'T BLOG, https://www.clearpointstrategy.com/sunshine-laws/.

46. Gerber, *supra* note 20, at 41.

Exceptions to public record laws reflect those found in FOIA, but vary in breadth among states.[47] Like the burden in FOIA, state law requires the agency from whom disclosure is sought to demonstrate that the information requested is exempt from public access by virtue of that state law's specifically legislated exemptions.[48] Because both FOIA and state law have legislated exemptions pertaining to personal privacy and security interests, it would appear that agencies could utilize an extant exception to protect reproductive health care service providers from disclosure of their personal data. Indeed, this would be possible, and has been done,[49] but the means and process of doing so is extremely burdensome on state and local agencies, and the success of utilizing a potentially applicable exception would ultimately rest on the discretion of the Office of Open Records and the state judiciary.[50] For this reason, this paper advocates for the creation of an express exemption in state public record laws for reproductive health care service providers given the known threats against their physical integrity by the release of personal identifying information.[51] The reasoning behind why an explicit blanket exemption is the best approach in light of current models of law is explained in Part III. The various types of legislation enacted to protect an individual's right to privacy and security is assessed below.

II. GROWTH IN RECOGNITION OF THE RIGHT TO PRIVACY

Legislation and policy have already been implemented within the United States, and around the world, in order to balance a recognized right to personal privacy and security against the value of transparency within the government and other public matters. These measures include, for example, confidentiality provisions and programs aimed at providing enhanced protections for victims of domestic violence, address confidentiality programs for reproductive health care service providers, and laws aimed at protecting

47. *See* 65 PA. CONS. STAT. § 67.708 (b) (2009) (listing 30 exceptions to disclosure of the Pennsylvania Right-to-Know Law); TEX. GOV'T CODE ANN. §§ 552.101-552.160 (listing more than 60 exceptions to disclosure).

48. *See, e.g.*, 65 PA. CONS. STAT. § 67.708.

49. *See* Crocco v. Pa. Dep't. of Health, 214 A.3d 316, 319-20 (Pa. Commw. Ct. 2019) (upholding the Department of Health's redaction of professional license numbers and names of health care practitioners and leadership in non-hospital abortion facilities under the personal security exception of the Right-to-Know Law, 65 PA. CONS. STAT. § 67.708 (b)(1)(ii)).

50. *See Crocco*, 214 A.3d at 327 ("The Court intends this holding [permitting the redaction of names and license numbers of health care practitioners and leadership in non-hospital abortion facilities] to be rare and limited to the unusual circumstances established by the extensive record in this case.").

51. *See, e.g.*, NAF 2018 statistics, *supra* note 6, at 4-6, 10.

individuals' online personal data. These types of legislative efforts show how lawmakers have recognized the threats to security and integrity that disclosure of personal information can have on individuals, and thus, have sought to strike the proper balance among competing interests through diverse legislative measures. Below we review these programs and provisions to analyze their strengths and weaknesses, and determine how they may need to be modified in the context of reproductive health care service providers to ensure the most effective balance between personal privacy, personal integrity, and democratic transparency.

A. *VAWA Grant Confidentiality Provision*

Because of known risks of harm faced by victims of domestic violence from their abusers, both federal and state law have been enacted to provide greater privacy protections so that abusers cannot locate their victims. In 1994, the Violence Against Women Act ("VAWA")[52] was enacted. It required the U.S. Postal Service to issue regulations to secure the confidentiality of addresses for both abused persons and domestic violence shelters.[53] VAWA marked the beginning of express recognition that domestic violence victims have a greater need for privacy because victims are already the target of an abuser.[54] Thus, extra protections are necessary to ensure that victims can live their lives free from the threat of harm their abusers pose.

In 1995, the National Criminal Justice Association prepared a report, "Confidentiality of Domestic Violence Victim's Addresses," as a resource for further action for protection.[55] In the report, the Director of the Violence Against Women's Office states:

---

52. Pub. L. No. 103-322 (codified in part as 42 U.S.C. §§ 13701-14040) [hereinafter VAWA 94]. For a description of VAWA 94 see Monica M. Modi et al., *The Role of Violence against Women Act in Addressing Intimate Partner Violence: A Public Health Issue*, 23 J. WOMEN'S HEALTH 253, 254-59 (2014), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3952594/ ("The VAWA act addresses domestic violence, dating violence, sexual assault, and stalking. . . . VAWA also makes [intimate partner violence] a federal crime when state lines are crossed. VAWA provides grants to states for programs that prevent violence against women or provide services for victims of violence.").

53. VAWA 94, *supra* § 40281 (a). These regulations were required to secure confidentiality for both individuals and shelters, with an exception of disclosure for law enforcement or other governmental purposes. *See id.* § 40281 (c).

54. Electronic Privacy Information Center, *Domestic Violence and Privacy*, https://epic.org/privacy/dv/#gr.

55. National Criminal Justice Association, *Confidentiality of Domestic Violence Victims' Addresses* (1995), https://www.ncjrs.gov/pdffiles1/Digitization/164064NCJRS.pdf.

> [I]nformation pertaining to the location of victims of violence is readily available through a variety of legitimate means. Postal services, voter registration records, motor vehicle records, school records, credit bureaus, computerized data bases, and caller ID are all sources of critical information that might, *in the wrong hands, lead to further abuse and criminal actions*.[56]

The report concluded that legislation providing victims of domestic violence with enhanced privacy protections can help these targeted individuals "reclaim a sense of peace and security in their lives."[57] Thus, "[p]ublic agencies should seek to adopt or improve *internal protocols* which govern the dissemination of personal information," and "[t]he impact of the Internet and related technological developments needs to be addressed."[58] Since enacted in 1994, VAWA has been reauthorized three times: in 2000, 2005, and 2013.[59]

During its 2005 reauthorization, the Act was amended to establish a grant program to enhance privacy protections for victims of domestic violence.[60] These amended provisions required institution recipients of VAWA grants to protect the personal information of their clients.[61]

---

56. *Id.* at Foreword (emphasis added).

57. *Id.*

58. *Id.* (emphasis added).

59. LISA N. SACCO, CONG. RESEARCH SERV., R45410, THE VIOLENCE AGAINST WOMEN ACT (VAWA): HISTORICAL OVERVIEW, FUNDING, AND REAUTHORIZATION 15-16 (2019), https://fas.org/sgp/crs/misc/R45410.pdf. VAWA's authorization expired on February 15, 2019; Whether it will be reauthorized has not yet been determined. *See* American Bar Association, *Violence Against Women Act Reauthorization Threatened* (2019), https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/may2019/vawa_update/.

60. Electronic Privacy Information Center, *VAWA and Privacy*, https://epic.org/privacy/dv/vawa.html [hereinafter EPIC].

61. *Id.* (citing 42 U.S.C. § 11383 (b)(2) (2006)). VAWA was later reauthorized in 2013 and amended to expand the definitions of various terms under the statute, further broadening its scope of coverage. Pub. L. No. 113-4 [hereinafter VAWA 2013]. VAWA 2013 also clarified that all VAWA grantees must document their compliance with the Act's confidentiality and privacy provisions. 34 U.S.C. § 12291 (b)(2)(G); National Network to End Domestic Violence, *The Violence Against Women Reauthorization Act of 2013: Summary of Changes*, http://www.ncdsv.org/images/NNEDV_VAWA-2013-Summary-of-changes.pdf ("All VAWA grantees must abide by strict confidentiality laws that are upheld and expanded in VAWA 2013. The confidentiality and privacy provisions in VAWA 2013 clarify that grantees must not disclose nor reveal or release any personally identifying information . . . regardless of whether the information has been encoded, encrypted, hashed, or otherwise protected.").

VAWA's confidentiality provision[62] requires all grantees and subgrantees[63]—such as nonprofits, universities, or government entities—to protect the confidentiality and privacy of persons to whom these entities are providing services.[64] This provision was designed to ensure the safety of victims of domestic violence, dating violence, sexual assault, and stalking by protecting their personal information.[65] The term "personal information" is defined broadly under the statute, and includes an individual's first and last name, their address, contact information, social security number, and "any other information. . . . that would serve to identify any individual."[66] The broad definition is meant to prevent the release of demographic data that could help identify a victim.[67] Thus, with some exceptions, grantees or subgrantees may not disclose the personal identifying information "collected in connection with services requested, utilized, or denied through grantees' and subgrantees' programs" without that individual's consent.[68]

Public policy supports extra layers of protection for victims of domestic violence, which includes nondisclosure of their personal information in order to "to ensure the safety of adult, youth, and child victims of domestic violence, dating violence, sexual assault, [and] stalking."[69] The confidentiality provision aims to prevent offenders from being able to track their vic-

---

62. 34 U.S.C. 12291 (b)(2) (2017).

63. U.S. Dep't of Justice, *OVW Grants and Programs*, https://www.justice.gov/ovw/grant-programs ("The Office on Violence Against Women (OVW) currently administers 19 grant programs authorized by [VAWA]. Four programs are 'formula,' meaning the enacting legislation specifies how the funds are to be distributed. The remaining programs are 'discretionary,' meaning OVW is responsible for creating program parameters, qualifications, eligibility, and deliverables in accordance with authorizing legislation. These grant programs are designed to develop the nation's capacity to reduce domestic violence, dating violence, sexual assault, and stalking by strengthening services to victims and holding offenders accountable.").

64. U.S. DEP'T OF JUSTICE: OFFICE ON VIOLENCE AGAINST WOMEN, FREQUENTLY ASKED QUESTIONS (FAQS) ON THE VAWA CONFIDENTIALITY PROVISION (34 U.S.C. § 12291 (B)(2)) 2 (2017), https://www.justice.gov/ovw/page/file/1006896/download ("Grantees and subgrantees 'covered' by the VAWA Confidentiality Provision must adhere to the requirements of that Provision . . . they may not disclose, reveal, or release personally identifying information or individual information collected in connection with services requested, utilized, or denied through grantees' and subgrantees' programs[.]").

65. *Id.*

66. 34 U.S.C. 12291 (a)(20).

67. EPIC, *supra* note 60.

68. 34 U.S.C. § 12291 (b)(2)(B). This section is subject to § 12291(b)(2)(C) and (D), which permits disclosure when compelled by statutory or court mandate, and for law enforcement purposes.

69. 34 U.S.C. 12291 (b)(2)(A).

tims in order to cause further harm.[70] Thus, VAWA's confidentiality provision evidences a legislative effort to strike the appropriate balance between personal privacy and security concerns and democratic transparency in the context of victims of violence *by requiring certain entities not to disclose their client's personal information.*

Nonetheless, VAWA has many limitations. Although this Act is a step in the right direction in terms of recognizing and providing targeted individuals greater protections, VAWA's confidentiality provision is weak because it does not provide across-the-board protection for victims. VAWA specifically calls upon "grantees and subgrantees" to comply with the confidentiality requirements, as opposed to a general requirement for everyone. Part of the reason for this lies in federalism constraints on the scope of national legislation. The United States Supreme Court has held that VAWA's provisions must be tailored to adhere to the principles of federalism,[71] limiting its power to prevent nondisclosure by state and local agencies. Therefore, state and local legislation is needed to ensure adequate privacy protections for all impacted individuals.

B. *State Address Confidentiality Programs*

State governments have sought to help fill some of VAWA's privacy gaps by establishing their own address confidentiality programs to protect victims of domestic violence.[72] These programs vary in breadth among states, but each seeks to prevent access to a domestic violence victim's location by shielding their address from the public. In New York, the Address Confidentiality Program allows victims of domestic violence to apply to the Secretary of State for a substitute address,[73] cost-free, and to shield their

---

70. Leslye E. Orloff, *VAWA Confidentiality: History, Purpose, DHS Implementation and Violations of VAWA Confidentiality Protections*, *in* EMPOWERING SURVIVORS: LEGAL RIGHTS OF IMMIGRANT VICTIMS OF SEXUAL ASSAULT (Leslye E. Orloff ed., 2013), https://www.lsc.gov/sites/default/files/LSC/pdfs/10.%20%20Appendix%20IX%20%20CH%203%20SA_Confidentiality_Final.pdf.

71. United States v. Morrison, 529 U.S. 598, 627 (2000); *see* Roger Pilon, *Violence Against Women Act Exceeds Federal Authority*, CATO INST. (Mar. 30, 2000), https://www.cato.org/publications/commentary/violence-against-women-act-exceeds-federal-authority.

72. As of today, 38 states have established Address Confidentiality Programs for victims of domestic violence. *See* Press Release, Betty McCollum, Representatives Announce Introduction of H.R. 4705, the Safe at Home Act (Oct. 21, 2019), https://mccollum.house.gov/media/press-releases/representatives-announce-introduction-hr-4705-safe-home-act.

73. Generally, a substitute address is a P.O. box assigned to the program participant by the designated department of which the program is operated. For instance, in

actual address.[74] The substitute address can be used when dealing with state and local agencies.[75] Furthermore, any first class, registered or certified mail sent to the substitute address will be forwarded to the program participant's actual (mailing) address by the Secretary of State.[76] This program ultimately provides one facet of an overall safety plan for victims of domestic violence.[77]

Wisconsin has a similar program. In Wisconsin, a person is eligible for participation in the Address Confidentiality Program[78] if the applicant is a resident of the state and one of the following: a victim of abuse,[79] a parent or guardian of a person who is a victim of abuse, or a resident of a household in which a victim of abuse resides, or if the individual attests that "he or she fears for his or her physical safety or for the physical safety of his or her child or ward."[80] The state's Department of Justice ("Department")[81] would then provide the applicant with an application form for participation in the confidentiality program, cost-free.[82] Once enrolled in the program, the Department would then provide the program participant with an assigned address that can be used when dealing with local and state agencies.[83] As with the New York program, the program participant is forwarded all first class, certified mail by the Department to his or her actual address. The Wisconsin address confidentiality program also provides for confiden-

---

New York, the substitute address is a Post Office box in Albany, New York. *See* New York State Dep't of State, *Address Confidentiality Program*, https://www.dos.ny.gov/acp/.

74. N.Y. EXEC. LAW § 108 (Mckinney 2019).

75. *Id.* § 108 (4)(a).

76. *Id.* § 108 (4)(c).

77. *Address Confidentiality Program*, *supra* note 73. The Address Confidentiality Program provides only two exceptions to nondisclosure of a participant's information: if the information is requested by a law enforcement agency for a legitimate law enforcement purpose or if the information is requested through a court order. *See* N.Y. EXEC. LAW § 108 (6).

78. WIS. STAT. § 165.68 (2018).

79. "Abuse" is defined under the program as "child abuse, domestic abuse, sexual abuse, stalking and/or trafficking." Wisconsin Dep't of Justice, *Safe at Home: Wisconsin Address Confidentiality Program Application*, https://www.doj.state.wi.us/sites/default/files/ocvs/Safe%20at%20Home/SAH%20Application_Updated%2001_209_FillablePDF.pdf.

80. WIS. STAT. § 165.68 (2).

81. The department in which the program is established varies among states.

82. WIS. STAT. § 165.68 (3).

83. *Id.* § 165.68 (4).

tial voting[84] if the program participant provides a municipal clerk with a valid written request.[85]

States like New York and Wisconsin have established address confidentiality programs because victims of domestic violence are targeted individuals who face a greater risk of harm than others in society.[86] Therefore, given their unique situation, enhanced protections must be put in place to address this magnified threat of harm. Significantly, other states, like California and New Jersey have adopted similar address confidentiality programs for victims of domestic violence, but have expanded them to incorporate reproductive health care workers as well. These two address confidentiality programs enable state and local agencies to respond to requests for public records without disclosing the actual address of reproductive health care service patients and providers.[87] California's Address Confidentiality for Reproductive Health Care Service Providers, Employees, Volunteers, and Patients went into effect in 2003, while New Jersey recently amended its address confidentiality program for victims of domestic violence to include victims of sexual assault and stalking, and "reproductive health service patients and providers" in 2019.[88] The programs seek to protect those affiliated with reproductive health care services from threats of harm that have become widespread within this field of care. California's Legislature declared:

> Persons and groups that oppose reproductive rights attempt to stop the provision of legal reproductive health care services by threatening reproductive health care service providers, clinics, employees, volunteers, and patients. The names, photographs, spouses' names, and home addresses of these providers, employees, volunteers, and patients have been posted on Internet Web sites. From one Web site list that includes personal information of reproductive health care service

84. *Id.* § 165.68 (5)(d).

85. *Id.* § 6.47 (2) ("To be valid, a request under this subsection must be accompanied by a copy of a protective order that is in effect, an affidavit . . . that is dated within 30 days of the date of the request, confirmation from the department of justice that the person is a program participant, as provided under s. 165.68 (4)(c), a statement signed by the operator or an authorized agent of the operator of a shelter that is dated within 30 days of the date of the request and that indicates that the operator operates the shelter and that the individual making the request resides in the shelter, or a statement signed by an authorized representative of a domestic abuse victim service provider or a sexual assault victim service provider under sub. (1) (am) 4. that is dated within 30 days of the date of the request.").

86. *See* N.Y. EXEC. LAW § 108 (Mckinney 2019); WIS. STAT. § 165.68 (2)(a).

87. *See* CAL. GOV'T CODE § 6215 (West 2003); N.J. REV. STAT. § 47:4-2 (2019).

88. *Id.*

> providers, seven persons have been murdered and 14 have been injured. As of August 5, 2002, there are 78 Californians listed on this site. The threat of violence toward reproductive health care service providers and those who assist them has clearly extended beyond the clinic and into the home.[89]

The California Act uses the term "[r]eproductive health care services provider, employee, volunteer, or patient," which is defined as "a person who obtains, provides, or assists, at the request of another person, in obtaining or providing reproductive health care services, or a person who owns or operates a reproductive health care services facility."[90] The legislation establishing California's program is just one of the governing laws of California's "Safe at Home" confidential address program administered by the California Secretary of State's office.[91] Safe at Home offers reproductive health care workers and victims of domestic violence, stalking, sexual assault, human trafficking, and elder abuse, a substitute mailing address to receive first class, certified, and registered mail.[92] More recently, in 2016, California expanded Safe at Home's protections by enacting legislation prohibiting individuals and businesses from publicly posting on the Internet the home address of a program participant or their family members.[93] To become a program participant of Safe at Home, each individual must complete a "Safe at Home Enrollment Application"[94] with an application assistant at a pre-identified enrolling agency.[95] The enrolling agency application assistant then mails completed forms to a specified address for approval by

---

89. CAL. GOV'T CODE § 6215 (c).

90. *Id.* § 6215.1.

91. Alex Padilla: California Sec'y of State, *Safe at Home*, https://www.sos.ca.gov/registries/safe-home/.

92. *Id.*

93. CAL. GOV'T CODE § 6215.10; NARAL, *State Laws: California*, https://www.prochoiceamerica.org/state-law/california/.

94. California Sec'y of State, *Safe at Home Enrollment Application*, https://sah.cdn.sos.ca.gov/forms/sample-enrollment-application2.pdf.

95. An "application assistant" helps applicants determine whether they are eligible to participate in Safe at Home and explain to applicants how Safe at Home can be a part of their overall safety plan. Application assistants can be found at an enrolling agency. An "enrolling agency" is an agency that has been designated to provide application assistance and services to those seeking to apply to the Safe at Home program. A list of these enrolling agencies can be found online: *See* Alex Padilla: California Sec'y of State, *Where to Find Enrolling Agency*, https://www.sos.ca.gov/registries/safe-home/where-find-enrolling-agency/.

the Secretary of State or an agent thereof.[96] Since the program was established in 1999, Safe at Home has helped protect over nine thousand targeted individuals, including reproductive health care workers.

New Jersey's Address Confidentiality Program, modeled after California's "Safe at Home" law, also aims to help targeted individuals who fear for their safety keep their actual addresses confidential.[97] New Jersey's Program was initially intended to assist victims of domestic violence who have relocated in their effort to keep batterers from finding them.[98] New Jersey's Legislature recently amended its confidentiality program in 2019 to include "reproductive health service patients and providers."[99] The New Jersey Senate unanimously passed the bill expanding the State's Address Confidentiality Program to include victims of sexual assault and stalking, and reproductive health care workers 37-0-0, and the bill passed the Assembly by a 75-0-0 vote.[100]

New Jersey's Legislative findings and declarations states: "The Legislature finds that persons attempting to escape from actual or threatened domestic violence, stalking, or sexual assault, and reproductive health service patients and providers may establish new addresses to prevent their assailants or other individuals from finding them."[101] The New Jersey Act defines "reproductive health service provider" as "a hospital, clinic, physician's office, or other facility that provides reproductive health services, including an employee, a volunteer, or a contractor of the provider."[102] The law has been perceived by advocates as "a necessary measure to protect victims of abuse and reproductive health care service patients and workers amidst national attacks on abortion clinics and providers."[103] The NAF Violence and Disruption report reveals that, in 2018, abortion clinics nationwide faced a record number of picketing and trespassing incidents.[104] Clinics and staff also faced increased rates of obstruction, vandalism, and online hate speech.[105] The increase in anti-abortion rhetoric by the Trump administra-

---

96. The enrolling agency application assistant must mail completed forms and required documents to: Safe at Home, P.O. Box 846, Sacramento, CA, 95812. *See Safe at Home Enrollment Application*, *supra* note 94.

97. N.J. REV. STAT. §§ 47:41–47:4-6 (2019).

98. State of New Jersey Dep't of Children and Families, *Domestic Violence Services*, https://www.nj.gov/dcf/women/domestic/dvawarenessmonth.html.

99. N.J. REV. STAT. §§ 47:4-2–47:4-6.

100. Insider NJ, *supra* note 6.

101. N.J. REV. STAT. § 47:4-2.

102. *Id.* § 47:4-3.

103. Insider NJ, *supra* note 6.

104. *Id.*; NAF 2018 statistics, *supra* note 6, at 2-3, 10.

105. NAF 2018 statistics, *supra* note 6, at 1; Insider NJ, *supra* note 6;

tion and the unsettling number of state laws restricting or banning abortion care[106] has ultimately set the stage for anti-abortion extremists to amplify their intimidating tactics.[107] New Jersey's efforts to amend its address confidentiality program to include "reproductive health service patients and providers" shows how it has sought to combat the very real danger anti-abortion extremists pose to these individuals by permitting nondisclosure of certain personal information. Moreover, both California and New Jersey's efforts to expand their address confidentiality programs to include reproductive health care service providers shows state recognition of the need for legislative responses aimed at addressing the heightened threat of harm these targeted individuals face.

Although California and New Jersey were right to acknowledge and address the increased threat of harm to reproductive health care service providers, the utilization of Address Confidentiality Programs is not enough. Address confidentiality programs were tailored to protect victims of domestic violence and abuse, which is individualized in nature. Domestic violence does not happen to only one category of people—victims are found across a spectrum of professions and diverse backgrounds, with no one common feature that can be used to predict who will be abused.[108] More generally, domestic violence occurs due to a struggle of power and control between the victim and their abuser.[109] Therefore, address confidentiality programs require individual requests or applications in order to work

---

106. As many as 25 abortion bans have been enacted in 2019 alone. *See* Elizabeth Nash et al., *State Policy Trends at Mid-Year 2019: States Race to Ban or Protect Abortion,* GUTTMACHER INST. (July 1, 2019), https://www.guttmacher.org/article/2019/07/state-policy-trends-mid-year-2019-states-race-ban-or-protect-abortion.

107. New Jersey abortion clinics have reported four invasions in 2019 alone. *See* Press Release, Insider NJ, Governor Murphy Signs Bill to Expand Address Confidentiality Program to Include Sexual Assault Survivors and Reproductive Health Patients and Workers (July 19, 2019), https://www.insidernj.com/press-release/governor-murphy-signs-bill-expand-address-confidentiality-program-include-sexual-assault-survivors-reproductive-health-patients-workers/.

108. *See, e.g.*, National Coalition Against Domestic Violence, *Dynamics of Abuse*, https://ncadv.org/dynamics-of-abuse ("Anyone can be a victim of domestic violence. There is no "typical victim." Victims of domestic violence comes from all walks of life, varying age groups, all backgrounds, all communities, all education levels, all economic levels, all cultures, all ethnicities, all religions, all abilities, and all lifestyles."); Melinda Smith & Jeanne Segal, Domestic Violence and Abuse, HELPGUIDE (last updated June 2019), https://www.helpguide.org/articles/abuse/domestic-violence-and-abuse.htm ("Domestic violence and abuse can happen to anyone; it does not discriminate.").

109. *Dynamics of Abuse*, *supra* ("Every relationship differs, but what is most common within all abusive relationships is the varying tactics used by abusers to gain and maintain power and control over the victim.").

as a practical matter because there is no sure way to know who a victim will be. This is different from reproductive health care service providers, who are a pre-identified and limited group of persons that we know are more likely than others to face threats of harm because of their occupation.[110] Because these two targeted groups are not in identical situations, the legislative response to the threats of harm they face must be unique to be effective.

C. *Personal Security Exception*

A third way that lawmakers have sought to protect targeted individuals from the dangers of disclosure of their personal identifying information is through case-by-case invocation of general personal security and safety exceptions. As discussed above, variations of public record laws permit agencies to utilize an exception to disclosure if the requested information would endanger the safety or personal security of an individual.[111] Under these exceptions, the burden rests on the agency to show that the applicable standard of harm has been met to permit nondisclosure.[112] Although these types of exceptions have been used primarily to protect correctional officers and other members of law enforcement,[113] they have, on occasion, been used to protect other individuals—including reproductive health care service providers.[114]

In one recent case, *Crocco v. Pennsylvania Department of Health*, the Commonwealth Court of Pennsylvania held that Pennsylvania reproductive health care service facilities were entitled to redact reproductive health care service providers' personal information under Pennsylvania's "personal security exception."[115] The case was brought by Jean Crocco, an elderly female staff member of the Pro-Life Action League,[116] after her request for

---

110. *See generally* note 6 *supra*.

111. *See, e.g.*, 65 PA. CONS. STAT. § 67.708 (b)(1)(ii) (2009) (providing that information is exempt from access by a requester if it "would be reasonably likely to result in a substantial and demonstrable risk of physical harm to or the personal security of an individual."); N.Y. PUB. OFF. LAW § 87 (2)(f) (McKinney 2020) ("Each agency shall . . . make available for public inspection and copying all records, except that such agency may deny access to records or portions thereof that . . . if disclosed could endanger the life or safety of any person[.]").

112. *See, e.g.*, Crocco, 214 A.3d at 321.

113. *Id.* at 325; Asian Am. Legal Defense & Educ. Fund v. New York City Police Dep't., 964 N.Y.S.2d 888 (N.Y. Sup. Ct. 2013).

114. *See Crocco*, 214 A.3d. at 326.

115. *Id.*

116. The Pro-Life Action League is an anti-abortion extremist organization founded by Joseph Scheidler in 1980. The organization's sole mission is to end abortion

"the most recent applications/reapplications for registration and licensing (if applicable) for all the non-hospital abortion facilities in PA" was partially denied.[117] The information withheld included the names and license numbers of health care practitioners (physicians, medical directors, and directors of nursing) and the names of leadership (administrators, owners, trustees, board members).[118] Ms. Crocco and the Pro-Life Action League had previously sued the Illinois Department of Health in 2016 to get unredacted abortion clinic records.[119] There, the agency ultimately consented to provide the names and license numbers of clinic owners, physicians and medical staff.[120] Unlike the outcome in Illinois, the Commonwealth Court of Pennsylvania in *Crocco* affirmed the Office of Open Record's final determination upholding the Department of Health's redaction of professional license numbers and names of individuals on abortion facility applications under the personal security exception of the Pennsylvania Right-to-Know Law ("RTKL").[121] The court stated:

> Providers' submissions contain specific averments of actual harm threatened to those serving abortion facilities. The shared characteristic is the performance of services to abortion facilities in some capacity. The evidence demonstrates that such service entails certain security risks. There is no evidence refuting this commonality. . . . Moreover, the RTKL *expressly recognizes categorical application of an exception based on the services an individual performs for a certain type of entity*. For example, Section 708(b)(6)(i)(C) of the RTKL provides a "blanket exemption" to home addresses of judges and law enforcement as "at-risk individuals" based on the functions they serve. The reason for the blanket exemption "*is to reduce the risk of physical harm/personal security to these individuals that may arise due to the nature of their job duties*. . . . We acknowledge that this

---

and is known for its "dynamic" pro-life activism. *See* Pro-Life Action League, *About the Pro-life Action League*, https://prolifeaction.org/about/.

117. Brief for Respondents Pennsylvania Department of Health et al. at 4, Crocco v. Pa. Dep't of Health, 214 A.3d 316 (Pa. Commw. Ct. 2019).

118. *Crocco*, 214 A.3d at 319.

119. Complaint for Injunctive and Declaratory Relief, Pro-Life Action League v. Illinois Dep't of Health, 2016-CH-06918 (Ill. Cir. Ct. 2016).

120. Marie McCullough, *Antiabortion Activist Sues to Get Pennsylvania Providers' Identities*, PHILA. INQUIRER (June 7, 2019), https://www.inquirer.com/health/abortion-clinics-pennsylvania-provider-lawsuit-20190607.html ("After [Jean Crocco, a staff member of the anti-abortion extremist group the "Pro-Life Action League,"] sued the Illinois Department of Health to get unredacted abortion clinic records, the agency consented to provide the names and any license numbers of clinic owners, physicians and medical staff.").

121. *Crocco*, 214 A.3d at 318-19.

> Court has not upheld the withholding of names alone under the personal security exception, except when presented with risks inherent in prison settings. Allowing the redaction of names, even of private individuals, is *rarely permitted*. However, *given the allegations of significant harm to individuals who serve abortion providers in some capacity, application of the security exception is warranted*.[122]

In its determination, the *Crocco* court found that the statistical evidence—the NAF 2018 Violence and Disruption Statistics[123]—corroborated the allegations of harm that befalls providers when their personal identifying information is released.[124] These statistics track and document incidents of violence and harm to providers nationwide. The *Crocco* court found this nationwide report was able to "buttress claims of actual harm and demonstrable risk to personal security of individuals who serve abortion facilities in some capacity," and "show risks or the likelihood of harm based on past incidents of harm."[125] Therefore, the court found that there was sufficient evidence of a real risk of harm to those who serve reproductive health care service facilities, entitling them to redaction of not only their addresses, but names as well.[126]

Although the personal security exception found in the Pennsylvania RTKL was successfully utilized in *Crocco* to justify nondisclosure, the *Crocco* court stated: "The Court intends this holding to be rare and limited to the unusual circumstances established by the extensive record in this case."[127] This is particularly concerning because the road to getting to the outcome in *Crocco* was extremely burdensome for the agencies. Records in an agency's possession are presumed public unless exempt under an exception of the RTKL, a privilege, or another law.[128] The burden of proving that a record of an agency is exempt from public access falls upon the agency receiving the request,[129] and direct interest participants are also subject to this burden to prove any exemptions they assert.[130] Thus in order to protect the reproductive health care service providers from the harms of disclosure, the Department of Health (Respondent) and the ten reproductive health care

---

122. *Id.* at 325 (using the term "abortion providers" when referring to the respondent agencies) (internal citations omitted) (emphasis added).

123. NAF 2018 statistics, *supra* note 6.

124. *Crocco*, 214 A.3d at 324.

125. *Id.*

126. *Id.* at 326.

127. *Id.* at 327.

128. *Id.* at 320 (citing 65 PA. CONS. STAT. § 67.305 (a) (2009)).

129. *Id.* at 321 (citing 65 PA. CONS. STAT. § 67.708 (a)(1)).

130. *Id.* (citing Global Tel*Link Corp. v. Wright, 147 A.3d 978 (Pa. Commw. Ct. 2016)).

service facilities who joined as direct interest participants[131] had to utilize their time and resources in order to show "actual or real and apparent" risk of harm that would result from disclosure.[132] Although these entities were able to build an "extensive" record,[133] agencies in similar positions in the future should not have to undergo this heavy task in order to combat requests made under state public record laws. Requiring agencies to prove a real risk of harm that we already know exists anytime a similar situation arises is unnecessarily burdensome. Moreover, the agencies were only given the opportunity to prove an exception applied in *Crocco* because the requested agency *itself* made the initial "correct" decision to redact the reproductive health care service providers' personal information in the first place. If the agency had chosen not to do this, then the information would have been disclosed and the reproductive health care service providers would be the ones who suffered the consequences.

D. *Blanket Exemption of Disclosure*

Although never yet applied to reproductive health care service providers, a fourth way lawmakers have sought to protect targeted individuals from the dangers of disclosure of their personal identifying information is through the legislation of a "blanket exemption" for a defined group of impacted individuals. Lawmakers have the ability to enact legislation that expressly recognizes categorical application of an exemption based on the services an individual performs for a certain type of entity.[134] For instance, as discussed in *Crocco*, Pennsylvania's RTKL has an explicit blanket exemption for law enforcement officers and judges, exempting their home address from the state's disclosure laws.[135]

By providing this blanket exemption, Pennsylvania's General Assembly recognized that the home addresses of these "at-risk individuals" should

---

131. Ten agencies joined as direct interest participants: Drexel University d/b/a Drexel ob/gyn Associates of Feinstein, Delaware County Women's Center, Mazzoni Center Family and Community Medicine, Planned Parenthood Keystone, Planned Parenthood Southeastern Pennsylvania, Berger & Benjamin, Allegheny Reproductive Health Center, Allentown Women's Center, Philadelphia Women's Center and Planned Parenthood of Western Pennsylvania. *Id.* at 319.

132. *Id.* at 324 ("While the RTKL does not define 'substantial and demonstrable,' we interpret this language to mean 'actual or real and apparent.'").

133. *Id.* at 327.

134. *See, e.g.*, 65 PA. CONS. STAT. § 67.708 (b)(6)(i)(C) (providing a "blanket exemption" to home addresses of judges and law enforcement).

135. 65 PA. CONS. STAT. § 67.708 (b)(6)(i)(C).

not, and will not, be subject to disclosure.[136] "[T]he purpose of this unconditional protection afforded to the home addresses of law enforcement officers and judges [in Pennsylvania] is to reduce the risk of physical harm/personal security to these individuals that may arise due to the nature of their job duties."[137] The exemption goes so far as to preclude the disclosure of these individuals' home addresses even if the requester is seeking the address of an individual who is not a judge or law enforcement officer, but resides at the exempt home address (i.e., a family member or beneficiary of a judge or law enforcement officer).[138]

Because there is a blanket exemption for the home addresses of judges and law enforcement officers in Pennsylvania, these particular categories of people do not have to depend on the discretion of agency members to protect that piece of their personal information. Nor do these individuals need to take efforts to opt-in to some sort of program for them to be given protection under the law. Instead, the lawmakers in Pennsylvania took into consideration the on-going threat of harm these individuals face due to the nature of their employment, and chose to recognize this reality explicitly in their public record law.[139]

Most other states have not yet established blanket exemptions for certain professions, and, instead, rely on their personal security or safety exceptions to protect individuals in positions which are extremely vulnerable to threats of harm.[140] As discussed above,[141] this choice of protection is inadequate because it opens the doors to demanding litigation and relies too heavily on the discretion and forethought of individual agencies. In contrast, an explicit blanket exemption, which doesn't give agencies the opportunity to disclose certain information to begin with, appears to be the most efficient way to actually protect the personal information of a limited category of people under the law.

E. *Individual Opt-in of all Disclosure*

A fifth way to protect privacy—more common in Europe than in the United States—is the enactment of laws that prevent any disclosure of personal identifying information of individuals without that individual's consent. Such laws require individuals to *opt-in* to disclosure rather than

136. State Emp's. Ret. Sys. v. Fultz, 107 A.3d 860, 866-67 (Pa. Commw. Ct. 2015).

137. *Id.* at 867.

138. *Id.*

139. *See id.*

140. *See, e.g.,* note 11 *supra.*

141. *See generally* Part ii (3) *supra.*

requiring agencies to determine on the basis of exemptions or exceptions whether to withhold personally identifying information.

European Union ("EU") nations, for example, have taken the lead in enacting legislation aimed at protecting the privacy of individuals and limiting what personal information can be gathered and displayed online. The European Union's landmark privacy law, the General Data Protection Regulation ("GDPR"),[142] standardizes data protection law across all 28 countries of the European Union and imposes strict rules on controlling and processing personally identifiable information.[143] It also extends the protection of personal data and data protection rights by giving control back to EU residents over their personal data.[144] The law grants EU citizens several rights and protections, including the right to be informed about how their personal data is being used, the right to have any misuses rectified, and the right to be forgotten.[145]

"Personal data" is defined broadly under the GDPR to include "any information relating to an identified or identifiable person."[146] Under this law, all organizations that process personal data of individuals in the EU are required to put in place certain protections and disclose more information about what data they collect.[147] For instance, companies are required to ask for consent in plain language before collecting or using a person's data—meaning, the person will be asked to "opt-in" to collection or use of their personal data.[148] Companies must also explain how a person's personal data

142. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) [hereinafter GDPR].

143. *Id.*; Kris Lahiri, *What Is General Data Protection Regulation?,* FORBES (Feb. 14, 2018), https://www.forbes.com/sites/quora/2018/02/14/what-is-general-data-protection-regulation/#73b03d4c62dd.

144. Lahiri, *supra*; Elizabeth Schulze, *The US Wants to Copy Europe's Strict Data Privacy Law – But Only Some of It*, CNBC (May 23, 2019), https://www.cnbc.com/2019/05/23/gdpr-one-year-on-ceos-politicians-push-for-us-federal-privacy-law.html.

145. GDPR, *supra* note 142, Ch. 3, arts. 12-23; Bernhard Warner, *Online-Privacy Laws Come With a Downside,* ATLANTIC (June 3, 2019), https://www.theatlantic.com/ideas/archive/2019/06/europes-gdpr-elevated-privacy-over-press-freedom/590845/.

146. Human Rights Watch, *The EU General Data Protection Regulation* (June 6, 2018), https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation# [hereinafter "HRW GDPR"]. This definition covers online and device identifiers such as, IP addresses, cookies, or device IDs, and also location data, user names, and pseudonymous data. *Id.*

147. *Id.*

148. *Id.*

is used, shared, and stored,[149] and individuals have the right to object to the use of their personal data at any time.[150] Special protections are applied to "sensitive" data, including information revealing someone's racial or ethnic origin, political opinions, religious or philosophical beliefs, data about health, etc.[151]

These enhanced protections are meant to safeguard individuals from unnecessary data collection, use of data in unanticipated ways, and biased algorithmic decision-making, based on the idea that personal data is linked to individuals' private lives and can reveal intimate details of their "thoughts, beliefs, movements, associates, and activities."[152] The GDPR ultimately aims to limit or prevent abusive intrusions into people's private lives through their personal data.[153]

Brazil, Japan, South Korea, and Israel have also set out to follow Europe's lead: Brazil has introduced a bill which closely mirrors the EU's new regulations, Japan has passed a data protection law creating a new independent online privacy board, South Korea is considering new privacy rules, and Israel has adopted updated requirements for disclosures of specified data breaches.[154] Although the United States currently has no federal data privacy legislation, discussion on the topic has increased due to this increasingly global push for data protection and online privacy from other countries.[155] In 2018, one day before the GDPR took effect, Democratic Senators introduced a resolution encouraging companies to apply European privacy protections included in the GDPR to U.S. citizens.[156] Moreover, some states, like California—which has enacted the California Consumer Privacy Act[157]—have already recognized the need for greater privacy protections with regard to collecting and disclosing personal data.

---

149. GDPR, *supra* note 142, Ch. 3, art. 13; HRW GDPR, *supra* note 146.

150. HRW GDPR, *supra* note 146.

151. *Id.*

152. *Id.*

153. *Id.*

154. Adam Satariano, *G.D.P.R., New Privacy Law Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES, May 25, 2018, at A1.

155. S. Res. 523, 115th Cong. (2017-2018); Juliana De Groot, *What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019*, DIGITALGUARDIAN: DATAINSIDER (Dec. 2, 2019), https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection ("The conversation [on federal data privacy] took a high profile turn with the congressional hearings of Facebook founder Mark Zuckerberg.").

156. S. Res. 523, *supra*; Satariano, *supra* note 154.

157. CAL. CIV. CODE §§ 1798.100-1798.199 (West 2020).

The rise of personal privacy protections around the world is evidence of a newfound global movement in which individual interests are held on a higher pedestal than in previous years in order to combat the powerful reach of technology in this digital age. The GDPR and subsequent similar legislation support nondisclosure of reproductive health care service provider's personal identifying information because they demonstrate a general push for personal privacy interests in lieu of competing public interests.

However, without more, these protections are undesirable for reproductive health care service providers. Indeed, such laws provide for numerous exceptions. The GDPR, for example, permits organizations to obtain and use an individual's personal data without consent if the entity's "legitimate interests" outweigh a person's rights and freedoms.[158] Some "legitimate interests" that entities can assert include fraud prevention, internal administration, information security, and even direct marketing.[159] The "legitimate interests" provision[160] therefore leaves open the opportunity for EU member states to interpret the provision in a way that allows data collectors and entities to avoid seeking consent in many situations.[161] This type of unchartered protection which allows for broad categories of exceptions for individual consent to the collection of personal data would ultimately result in inadequate protection for reproductive health care service providers.

III. The Need for a Blanket Exemption for Reproductive Health Care Service Providers

Experiences in the United States and globally with the five approaches discussed above show that the only approach that will work effectively to best balance the right to public information and the need to protect the security of reproductive health care service providers is a blanket exemption of disclosure for their personal identifying information.

The first approach, enacting federal legislation, like VAWA, would not provide sufficient protections for reproductive health care service providers due to the Constitutional restraints placed on federal power.[162] Federalism limits Congressional power and its ability to command state agencies to comply with the federal law. Thus, relying on a federal law alone to protect providers would result in incomplete protection for all impacted individuals because state agencies may choose not to comply. Therefore, state and local legislation is necessary to ensure optimal privacy protections for providers.

158. HRW GDPR, *supra* note 146.
159. *Id.*
160. GDPR, *supra* note 142, Ch. 2, art. 6 (1)(f).
161. HRW GDPR, *supra* note 146.
162. *See generally supra* note 71.

The second approach, expanding state address confidentiality programs, is not the best option because these programs are not tailored to fit the needs of reproductive health care service providers—who are a unique category of people. Instead, address confidentiality programs were designed to protect victims of domestic violence and abuse, who are not confined to a pre-identified or limited group of persons. Thus, even though these programs—which require individuals to opt-in to nondisclosure—may make sense for victims of domestic violence, they do not cater to the particular needs of reproductive health care service providers.

Address confidentiality programs also provide insufficient forms of protection in the context of today because they do not shield individual names from disclosure. Given the massive reach of internet searches, and the influence of social media sites, it is easier than ever to find information on someone if you have their name.[163] Almost everyone has social media or has friends and family that use social media. Reproductive health care service providers and their families should not be penalized or excluded from a social phenomenon because of their profession or relation to someone in that profession. To permit the disclosure of providers' names would be to condemn reproductive health care service providers and their loved ones to real threats of harm, and arguably equivalent to directly disclosing their home address for anti-abortion extremists to come find them.

For these reasons, states' efforts to expand their address confidentiality programs to include reproductive health care service providers ultimately results in inadequate protections for this targeted group. Instead, providers should be given a means of protection from disclosure of personal identifying information that is tailored to the unique needs of this category of people. As discussed below, this may require explicit blanket exemptions.

The third approach, utilizing a personal security or safety exception, would not provide adequate protections for reproductive health care service providers. This approach may seem like the most appropriate option for providers because it has been successfully applied to prevent disclosure of their personal information in the past,[164] but the process of doing so is overly burdensome. The time and resources that agencies will waste in order to satisfy their burden of proof under one of these exceptions is unnecessary—especially since there is clear evidence a real risk of harm to

---

163. *See, e.g., Find out Personal Information about someone for free,* PEEP-LOOKUP, https://www.peeplookup.com/how-to-find-out-personal-information-about-someone-for-free; Mark Sullivan, *9 Sites that Find People and Their 'Sensitive' Information*, PCWORLD (Oct. 1, 2008), https://www.pcworld.com/article/151556/usesensitive.html.

164. *See* Crocco, 214 A.3d at 321.

providers already exists.[165] Therefore, providers need a layer of protection, such as a blanket exemption of disclosure, that does not require agencies to continuously prove that providers require protection in the form of nondisclosure under the law.

The fifth approach, enacting legislation similar to the GDPR, which calls for individuals to opt-in for all disclosure, is not a practical model of legislation for reproductive health care service providers. There are many flaws to the GDPR. Most notably, the Regulation has a "legitimate interests" provision—which allows EU member states to interpret the provision in a way that allows entities to avoid seeking individual consent in many situations.[166] Thus, in effect, this Regulation does not actually provide much protection for individuals. Therefore, reproductive health care service providers would still need to seek other options to ensure their information is protected, such as a blanket exemption.

Because reproductive health care service providers are a unique category of people who face real threats of harm from anti-abortion extremists, the best approach for protecting their personal information is to establish an explicit blanket exemption of disclosure. Without an explicit categorical exemption of disclosure for providers' personal information, agencies may not know that certain personal information, such as names, should be redacted or not disclosed under any specific exception or exemption. Moreover, a requester's motivation for making their request is not relevant in a determination for disclosure, and the intended use for the information may not be grounds for denial.[167] Thus, without realizing the risk of harm they are imposing on providers, agencies may consent to the release of certain personal information, placing providers in harms way.[168]

Any disclosure of information pertaining to this targeted group of people is dangerous because once a record is public for one, it is public for all.[169] In its decision regarding Ms. Crocco's request, the Commonwealth Court of Pennsylvania stated: "Although this particular requester may not pose a danger to the individuals whose names she seeks, once the information is deemed public, it is in the public domain and accessible to everyone

---

165. *See generally* note 6 *supra*.

166. GDPR, *supra* note 142, Ch. 2, art. 6 (1)(f); HRW GDPR, *supra* note 146.

167. *See, e.g.*, *Crocco*, 214 A.3d at 327 (citing *Padgett v. Pa. State Police*, 73 A.3d 644, 647 (Pa. Commw. Ct 2013)).

168. *See* McCullough, *supra* note 120 ("After [Jean Crocco, a staff member of the anti-abortion extremist group the "Pro-Life Action League,"] sued the Illinois Department of Health to get unredacted abortion clinic records, the agency consented to provide the names and any license numbers of clinic owners, physicians and medical staff.").

169. *Crocco*, 214 A.3d at 327 (citing *Padgett*, 73 A.3d at 647).

on the same basis."[170] The court went on to explain that protections may be warranted in cases where groups of individuals are targeted based on a function they perform or an entity they serve.[171]

We know from national and state statistics that this problem is widespread and that protections for reproductive health care service providers are necessary.[172] Thus, in light of the known threats of harm providers face as a consequence of their job, and the recent opinion in *Crocco*, state legislatures should seriously consider amending their public record laws to include a blanket exemption of disclosure for reproductive health care service providers' personal information. Public record laws were not intended to be a means by which individuals can obtain information to victimize other citizens—which is why certain exceptions or exemptions have been put in place.[173] Therefore, if we are actually going to strike the appropriate balance between the underlying "right to know" in a democratic society and the right to personal security and integrity, each state should establish a blanket exemption of disclosure to protect providers' personal information from abuse.

IV. OPERATIONALIZING A NEW BLANKET EXEMPTION UNDER STATE PUBLIC RECORD LAWS

What would such statutory exemptions look like? To be effective, such laws should be enacted at the state level and include three specific components to effectuate optimal protection. Below, each of those three components are discussed.

A. *Public record laws must provide an explicit blanket exemption for reproductive health care service providers*

First, states should be presented with specific bills for adoption that recognize an express statute exemption in their public record laws for all personal identifying information of reproductive health care service providers. Such a statutory exemption would include an express definition of who a "reproductive health care service provider" is, and what is considered "personal identifying information," "reproductive health care services," and a "reproductive health care service facility." Model language is included

---

170. *Id.*

171. *Crocco*, 214 A.3d at 325-27.

172. *See generally supra* note 6.

173. *See* Memorandum from Attorney General, *supra* note 18, at 2; *see also* 65 PA. CONS. STAT. § 67.708 (b)(6)(i)(C), (b)(1)(ii) (2009); N.Y. PUB. OFF. LAW § 87 (2)(f) (McKinney 2020).

below based on state-level legislation already in place to protect other professions susceptible to high risk of danger.

> **EXCEPTIONS.—** The following are exempt from access by a requester under this act:
>
> **(A)** The personal identifying information of a reproductive health care service provider[174]

The public record law would have to include definitions for the terms relevant to this blanket exemption.[175] For example:

> **DEFINITIONS.—**The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:
>
> "Reproductive health care service provider" means any owner, operator, contractor, agent, or employee of a reproductive health care service facility, or any person who provides or assists in the provision of reproductive health care.
>
> "Reproductive health care service facility" means a hospital, clinic, physician's office, or other licensed health care facility that provides reproductive health care services.
>
> "Personal identifying information" means the program participant's name or names, address or addresses, the name or names of the participant's employer, education, training, or other work activity, personal or work email addresses, personal or work telephone numbers, professional license numbers, social security number, and any other information that may be used to identify a person uniquely.
>
> "Reproductive health care services" means medical, surgical, counselling, or referral services relating to the human reproductive system, including services relating to pregnancy or the termination of a pregnancy, and transgender health services.

Lawmakers should refer to the terms and definitions found in this example when amending their public record laws to ensure an inclusive exemption.

---

174. *See* 65 PA. CONS. STAT. § 67.708 (b)(6)(i)(C) ("[T]he following are exempt from access by a requester under this act: . . . The home address of a law enforcement officer or judge.").

175. The definitions for "reproductive health care service provider," "reproductive health care service facility," and "reproductive health care services" are modeled after actual definitions used in both California and New Jersey's Address Confidentiality Programs. *See* CAL. GOV'T CODE § 6215.1 (West 2003); N.J. REV. STAT. § 47:4-3 (2019).

B. *Mandatory state and national reports/statistics showing the threat of harm to reproductive health care service providers*

Statutory provisions, like the sample one above, however, are not enough. Efforts likewise need to be made to increase public and agency awareness of the extent of threats to reproductive health care service providers. Thus, state and national agencies should publish regularized data and reports on the extent of the problem, tailoring additional efforts aimed at removing these threats.

The NAF annual reports and statistics[176] are a good example of current studies that disclose various instances of threats, violence, and destruction against reproductive health care service facilities and providers. State and national organizations and institutions should expand on these findings and narrow in on particular subjects in order to provide informative tools for change. These recommended reports and statistics should focus on how providers' personal information has been exploited and essentially harnessed as a weapon by anti-abortion extremists to target, intimidate, and victimize reproductive health care service providers. An increase in substantive reports that shine light on the intentional and malicious dissemination of personal information by anti-abortion extremists would bring a greater public awareness to the reality of this issue. Directives should be put in place at state and local levels to encourage or require annual or biannual publication of such reports.

C. *Internal protocols and training for local and state agencies*

Finally, internal protocols and trainings need to be developed to help agencies implement these exemptions. These internal protocols and trainings should ultimately develop and express a policy of nondisclosure when it comes to information pertaining to reproductive health care service providers. As discussed above,[177] under FOIA, whether a real threat exists is determined on an agency basis through *internal protocols and procedure*, taking into account precedent and context.[178] Personnel in state agencies should also be making a similar analysis, and thus, it is imperative they are given proper instructions on this particular area. Protocols and procedure on this topic should be provided to personnel in written and oral form, accom-

176. National Abortion Federation, *Violence Statistics & History*, https://prochoice.org/education-and-advocacy/violence/violence-statistics-and-history/.

177. *See generally* Part I *supra*.

178. *What are FOIA Exemptions?*, *supra* note 44 ("The FOIA authorizes agencies to withhold information when they reasonably foresee that disclosure would harm an interest protected by one of these nine exemptions.").

panied by mandatory trainings that push a policy of nondisclosure for this particular area. Agencies should also consider consulting with and seeking advice from a knowledgeable individual affiliated with a reproductive health care service facility who can explain important terms and definitions found in the state's blanket exemption. The scope of these terms, and who is covered under these definitions, will be important when deciding whether information may be disclosed or not.

Conclusion

Reproductive health care service providers are a discrete category of professionals, which have been, and still are, major targets for anti-abortion extremists. Anti-abortion extremists go to great lengths to obtain personal information about reproductive health care service providers and the easy accessibility of this information through public records has only aided in the victimization of this targeted group. We must work together to strike the appropriate balance between the purpose of enabling public access to information necessary for informed, participatory democracy, and the protection of personal security and integrity of reproductive health care service providers. Experience shows that the best approach to achieve this balance is through enacting a professional category exemption. It will only take small, smart changes like this to achieve effective change that could save lives and protect this targeted group.