To: Michael Kron, Oregon Sunshine Committee Chair

From: Ginger McCall, Oregon Public Records Advocate

Re: Survey of the treatment of personal information by federal and state public records laws, and by private businesses

Date: December 18, 2018

This informational report is provided to the Sunshine Committee to assist in its deliberation of certain personally identifiable information ("PII") exemptions to public records disclosure that are currently under consideration. The information in this report was compiled by the Office of the Public Records Advocate.

This report is divided into four sections, as follows:

Section I	Risks of Disclosure of Personally Identifiable Information
Section II	Privacy and Personally Identifiable Information Under the Freedom of Information Act
Section III	Personally Identifiable Information Under State Public Records Laws
Section IV	Selective Waiver of Conditional Exemptions

The report first summarizes risks posed by the release of personally identifiable information, particularly risks of three common practices: identity theft, doxing, and swatting. The ease with which information can be shared, traded, or sold online creates new problems, taking once obscure information and greatly increasing the risk of abuse.

The report next summarizes how other states and the Federal government approach the management and disclosure of PII, particularly personal contact information, under public records laws.

Finally, the report addresses the question of whether or not documents subject to conditional exemptions may be disclosed to one requester and not another.

Section I Risks of Disclosure of Personally Identifiable Information

Personally identifiable information (PII) is any information that can be used to distinguish or trace an individual's identity or is linked or linkable to an individual.[1] Information that can be used to distinguish or trace an identity includes name, Social Security number, and date and place of birth, whereas information that is linked or linkable to an individual includes medical, educational, financial, and employment information.[2] Oregon law defines "personal information" as a person's first and last name combined with certain other information (like Social Security number, driver license, or passport number; credit or debit card number and code or password;

[1] "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", report of the National Institute of Standards and Technology (NIST), Special Publication 800-122, April 2010, p. 2-1; https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

[2] *Id.*

data of physical characteristics such as fingerprint; health insurance numbers; or information about the person's medical condition or history), or any of those individual elements if the data alone is usable or would allow for identity theft.[3]

Private companies and government bodies necessarily gather PII for employees (such as home address, social security number for payment, financial information for direct deposit, medical information for leave and benefits, etc.), but many private businesses and government bodies also gather PII from other individuals who interact with the organization, including customers, individuals applying for benefits, and individuals who file complaints. Regardless of the source of the PII, because of the risks posed by disclosure, organizations must protect PII against unauthorized use, and often must notify consumers if the organization does not sufficiently protect PII. For instance, in Oregon, as in many states, state law requires businesses that own or license personal information to notify the consumer and the Attorney General after discovering a breach of security. ORS 646A.604. *See also* Cal. Civ. Code §§ 1798.83(a) et seq.; Idaho Code Ann. §§ 28-51-105(1) et seq.; Wash. Rev. Code Ann. §§ 19.255.010(1) et seq.; D.C. Code §§ 28-3852(a) et seq.; Tex. Bus. & Com. Code Ann. §§ 521.053(b) et seq.; Fla. Stat. Ann. §§ 501.171(4) et seq.

Data breaches have increased in severity and frequency over time.[4] According to the Identity Theft Resource Center (ITRC), there were more data breaches in 2017 than any year on record, and 44.7 percent more than in 2016, the previous record year.[5] Almost 179 million records were exposed by breaches in 2017, nearly five times more than were in 2016.[6]

The effects of PII disclosure or breach can be quite serious and long lasting, even if data is only exposed for a short time. Once a breach occurs, PII is often posted or sold on the "dark web," a marketplace for stolen data.[7] For permanent PII, such as medical history and social security number, or information that is difficult to change, such as social security number, bank account or home address, the victim may never be entirely secure from the effects of a single breach.

The inadvertent or unauthorized disclosure of PII may have significant costs to the individual whose information was exposed. Depending on the type of data available, an individual may suffer economic, social, or even physical harm.[8] Identity theft is one of the most common, and commonly understood, outcomes from the exposure of PII in a data breach.[9] Identity theft (also

---

[3] ORS 646A.602.
[4] "2017 Data Breach Year-End Review", report of the Identity Theft Resource Center (ITRC 2017); https://www.idtheftcenter.org/2017-data-breaches/.
[5] ITRC counts breaches for the following industries: banking/credit/financial, business, educational, government/military, and medical/healthcare. In 2017, business accounted for a majority of breaches, whereas in 2016 it accounted for a plurality. ITRC 2017; ITRC 2016. ITRC's annual breach reports also track breaches that do not involve sensitive PII but that reveal exposure of user names, email addresses, and passwords. ITRC 2017.
[6] *Id.*; ITRC 2016.
[7] Here's How Much Thieves Make by Selling Your Personal Data Online, Cadie Thompson, Business Insider, May 27, 2015, available at: https://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5.
[8] "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", report of the National Institute of Standards and Technology (NIST), Special Publication 800-122, April 2010, App. B-6; https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.
[9] "Identity Theft Statistics", Experian Report; https://www.experian.com/blogs/ask-experian/identity-theft-statistics/.

known as identity fraud) is defined as the unauthorized use of another person's personal information in a way that involves fraud or deception, typically for financial gain.[10] Identity theft can be extremely expensive, and can also damage a victim's credit or compromise her medical records.[11] Addressing and correcting damage resulting from identity theft may also require significant investments of time and money.[12]

Two more increasingly common abuses of PII are "doxing" (or "doxxing") and "swatting."

Doxing is the practice of publishing a person's private documents (or "dox") against the person's wishes.[13] Victims who are doxed become especially vulnerable to threats and harassment and are often forced to shut down online accounts,[14] change contact information, or even move.[15]

Doxing has become increasingly mainstream in recent years.[16] It is often used to exact revenge or to silence opponents.[17] For example, doxing became a popular weapon in the 2014 "GamerGate" controversy, an online movement purportedly concerned with ethics in video game journalism. In GamerGate, "mostly male video-game players began to publish personal information --- including home address and phone numbers --- for women in their community, typically journalists and game designers who they said were unfairly polarizing gaming culture."[18] Doxing became such a prevalent tool in GamerGate that well-known personalities refused to weigh in on the movement for fear of being doxed.[19]

Doxing is often a part of online vigilantism, as well, and frequently results in innocent parties facing threats and harassment. During the search for the Boston Marathon bombers, several innocent individuals were doxed online by internet users who were "investigating" the bombing.[20] Families of the falsely accused were harassed and targeted.[21] In the wake of the

---

[10] US DOJ Criminal Division; https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.
[11] *See* Footnote 33.
[12] *Id*.
[13] What Doxxing is and Why it Matters, The Economist Explains, Mar. 10, 2014, available at: https://www.economist.com/the-economist-explains/2014/03/10/what-doxxing-is-and-why-it-matters; How "Doxxing" Became a Mainstream Tool in the Culture Wars, Nellie Bowles, New York Times, Aug. 30, 2017, available at: https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html.
[14] Why People Ruin Others' Lives by Exposing All Their Data Online, Timothy Revell, New Scientist, Nov. 13, 2017, available at: https://www.newscientist.com/article/2152950-why-people-ruin-others-lives-by-exposing-all-their-data-online/.
[15] Blasey Ford Facing Online Threats, Doxing, Moves Out of Home, Elise Viebeck, *The Mercury News*, Sept. 18, 2018, available at: https://www.mercurynews.com/2018/09/18/blasey-ford-facing-online-threats-doxing-moves-out-of-home/.
[16] How "Doxxing" Became a Mainstream Tool in the Culture Wars, Nellie Bowles, New York Times, Aug. 30, 2017, available at: https://www.nytimes.com/2017/08/30/technology/doxxing-protests.html.
[17] When Studying Doxing Gets you Doxed, Damon McCoy, Huffington Post, May 1, 2018, available at: https://www.huffingtonpost.com/entry/opinion-mccoy-doxing-study_us_5ae75ec7e4b02baed1bd06cc.
[18] *Id*.; *see also* https://www.theguardian.com/technology/2014/oct/23/felicia-days-public-details-online-gamergate.
[19] *Id.*
[20] Body of Missing Student at Brown is Discovered, Jess Bidgood, New York Times, April 25, 2013, available at: https://www.nytimes.com/2013/04/26/us/sunil-tripathi-student-at-brown-is-found-dead.html.
[21] The Real Story of Sunil Tripathi The Boston Bomber Who Wasn't, Traci G. Lee, NBC News, June 22, 2015, available at: https://www.nbcnews.com/news/asian-america/wrongly-accused-boston-bombing-sunil-tripathys-story-now-being-told-n373141

Charlottesville white supremacist rallies, many activists took to social media to share photos of marchers and work to identify them.[22] One man, Professor Kyle Quinn, was wrongly identified as one of the white supremacists.[23] His address and contact information were published, his employer was contacted, and he was repeatedly threatened and harassed online.[24] Professor Quinn and his family were forced to leave their home.[25] After the shooting of Michael Brown by a police officer in Ferguson, Missouri, online vigilantes published the names and addresses of the county police chief's family, as well as the name of an entirely innocent individual whom they claimed had shot Mr. Brown.[26]

Doxing can also be motivated by political animosity. Two prominent recent examples of doxing occurred during the confirmation process of now Supreme Court Justice Brett Kavanaugh. In September a Twitter user posted the home address and phone number of Dr. Christine Blasey Ford, accuser of now Supreme Court Justice Brett Kavanaugh. This information was then copied and shared elsewhere on the Internet.[27] Since then, Dr. Ford has frequently been threatened and harassed, and has moved four times.[28] During the confirmation hearing process, several senators associated with the process were also doxed.[29] Their home addresses and contact information were published on Wikipedia.[30] A former congressional staffer was later arrested for this doxing.[31]

A few months later, in a politically motived doxing episode, Tucker Carlson, a prominent conservative commentator, was doxed.[32] Protesters later showed up at his home, threatened his family, and vandalized his property.[33]

There is a long history of government officials, in particular, being doxed.[34] Law enforcement officers have frequently been doxed by both online activists[35] and those under investigation.[36] In

[22] Kyle Quinn Hid at a Friend's House After Being Misidentified on Twitter as a Racist, Laura Sydell, NPR, August 17, 2017, available at: https://www.npr.org/sections/alltechconsidered/2017/08/17/543980653/kyle-quinn-hid-at-a-friend-s-house-after-being-misidentified-on-twitter-as-a-rac.
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] Anonymous Hackers' Efforts to Identify Ferguson Police Officer Create Turmoil, Nicole Perlroth, New York Times, Aug. 14, 2014, available at: https://www.nytimes.com/2014/08/15/us/ferguson-case-roils-collective-called-anonymous.html.
[27] A Troll Doxxed Christine Blasey Ford. Twitter Let Him Back on its Platform in Hours, Jesselyn Cook, Huffington Post, Sept. 20, 2018, available at: https://www.huffingtonpost.com/entry/troll-doxxed-christine-blasey-ford-twitter_us_5ba3ba6ee4b069d5f9d0ce92.
[28] Kavanaugh Accuser Christine Blasey Ford Continues Receiving Threats, Lawyers Say, Tim Mak, NPR, Nov. 8, 2018, available at: https://www.npr.org/2018/11/08/665407589/kavanaugh-accuser-christine-blasey-ford-continues-receiving-threats-lawyers-say
[29] *Ex-Democratic Staffer Charged with Posting Senators' Private Info*, Burgess Everett and Kyle Cheney, Politico, Oct. 3, 2018, available at: https://www.politico.com/story/2018/10/03/gop-senators-doxxing-arrest-868122.
[30] *Id.*
[31] *Id.*
[32] Police Launch Investigation After Antifa Activists Descend on Fox Host Tucker Carlson's Home, Brian Stelter, CNN, Nov. 8, 2018, available at: https://www.cnn.com/2018/11/08/media/tucker-carlson-protestors/index.html.
[33] *Id.*
[34] See e.g. Anonymous Hackers' Efforts to Identify Ferguson Police Officer Create Turmoil, Nicole Perlroth, New York Times, Aug. 14, 2014, available at: https://www.nytimes.com/2014/08/15/us/ferguson-case-roils-collective-called-anonymous.html.

response to law enforcement investigations into the group's hacking activities, Anonymous released the private information of more than 7,000 police officers.[37] In 2016, one hacker doxed nearly 30,000 government employees, including employees of the Federal Bureau of Investigation and Department of Homeland Security.[38] Locally, in Portland, during the summer of 2018, activists doxed employees of Immigration and Customs Enforcement, posting their home addresses and phone numbers, which resulted in threats of violence and harassment of these employees.[39]

As noted in one recent story regarding the doxing of 2,300 government employees, releasing the PII of government employees creates not only personal safety concerns, but also national security concerns because it allows foreign governments to identify and potentially target U.S. government workers.[40]

Another use of home address PII, and a favored tactic of the gamer communities online, is swatting, the practice of anonymously contacting emergency services to falsely report a serious or violent incident to draw large numbers of law enforcement or SWAT teams to a victim's home.[41] Swatting started among gamers who broadcast or stream their play live and who "swatted" their opponents because they, and their viewers, were able to watch the potentially violent result.[42] Swatting takes doxing to an automatically dangerous and violent level because law enforcement has no way of knowing the report is false, and responds to the call as if the violent threat is real. [43] Swatting has led to at least one death.[44] Celebrities are swatted regularly,

---

[35] *Id.*
[36] 'Topiary' Released on Bail, Identity Unclear, as Anonymous Reprisals Fall Flat, Kevin Fogarty, IT World, Aug. 1, 2011, available at: https://www.itworld.com/article/2740095/security/-topiary--released-on-bail--identity-unclear--as-anonymous-reprisals-fall-flat.html.
[37] *Id.*
[38] Hacker Doxed Nearly 30,000 Government Agents While You Were Watching the Superbowl, Bryan Clark, The Next Web, Feb. 8, 2016, available at: https://thenextweb.com/insider/2016/02/09/hacker-doxxed-nearly-30000-government-agents-while-you-were-watching-the-super-bowl/.
[39] Portland Activists Post Phone Numbers, Home Addresses of Ice Employees, Morgan Gstalter, The Hill, June 22, 2018, available at: https://thehill.com/blogs/blog-briefing-room/news/393692-portland-activist-posts-home-phone-numbers-addresses-of-ice; *see also* Ice Union Asks Portland Mayor for Police Protection, Anna Spoerre, The Oregonian, Aug. 1, 2018, available at: https://www.oregonlive.com/portland/index.ssf/2018/07/ice_asks_portland_mayor_for_po.html.
[40] The Dox of More than 2,300 Government Employees Might be Worse than We Thought, Lorenzo Franceschi Bicchierai, Motherboard, Nov. 6, 2015, available at: https://motherboard.vice.com/en_us/article/xyg8wa/the-dox-of-more-than-2300-government-employees-might-be-worse-than-we-thought.
[41] Federal Bureau of Investigation, Don't Make the Call: The New Phenomenon of 'Swatting', Feb. 4, 2008, https://archives.fbi.gov/archives/news/stories/2008/february/swatting020408; and Police Kill a Man at His Home While Responding to a Fake Call, Doug Criss, Carma Hassan, and AnneClaire Stapleton, CNN, Dec. 30, 2017, available at: https://www.cnn.com/2017/12/30/us/kansas-police-shooting-swatting/index.html.
[42] Everything You Need to Know About 'Swatting,' the Dangerous So-Called 'Prank' of Calling a Swat Team on Someone, Kaylee Fagan, Business Insider, June 5, 2018, available at: https://www.businessinsider.com/what-does-swatting-mean-2015-3
[43] *Id.*
[44] Police Kill a Man at His Home While Responding to a Fake Call, Doug Criss, Carma Hassan, and AnneClaire Stapleton, CNN, Dec. 30, 2017, available at: https://www.cnn.com/2017/12/30/us/kansas-police-shooting-swatting/index.html; Shooting Death in Video Game Leads to a Real One in Kansas, available at: http://www.cnn.com/2018/01/30/us/kansas-swatting-death-affidavit/index.html

but both swatting and doxing are increasingly used against formerly private people who speak out for or against a hot button issue and instantly become public figures.[45]

Section II Privacy and Personally Identifiable Information Under the Freedom of Information Act

- Privacy Under the FOIA, Generally

The Federal Freedom of Information Act ("FOIA") includes two separate exemptions that cover privacy. Exemption 6, protects information about individuals in "personnel and medical files and similar files" when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy."[46] Exemption 7(C) is limited to information compiled for law enforcement purposes, and protects personal information when disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy."[47]

Both personal privacy exemptions of the FOIA protect not only information which is inherently private, but also an "individual's control of information concerning his or her person."[48] Like Oregon's personal privacy exemptions, the FOIA incorporates a balancing test. In evaluating whether or not to withholding information under Exemption 6, agencies are required to conduct a four step analysis: 1.) Determine whether the information in question qualifies as "personnel, medical, [or] similar files,"[49] 2.) Determine whether there is a significant privacy interest in the requested information,[50] 3.) Evaluate the requester's asserted FOIA public interest in disclosure,[51] and 4.) Balance those competing interests to determine whether disclosure "would constitute a clearly unwarranted invasion of personal privacy." Courts have instructed agencies to default to a presumption of disclosure. [52]

The Supreme Court has found that Congress meant for the term "similar file" to be interpreted very broadly, holding that all information that "applies to a particular individual" meets the threshold requirement for Exemption 6.[53]

- Personally Identifiable Information Generally Protected Under FOIA

Courts have recognized a significant privacy interest under the FOIA in personally identifiable information as a person's name, address, image, computer user ID, phone number, date of birth,

[45] Boy Admits to 'Swatting' Ashton Kutcher, Justin Bieber, Alan Duke, CNN, Mar. 12, 2013, available at: https://www.cnn.com/2013/03/11/showbiz/kutcher-swatting-conviction/index.html
[46] 5 U.S.C. 552(b)(6).
[47] 5 U.S.C. 552(b)(7)(C).
[48] *DOJ v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989).
[49] 5 U.S.C. 552(b)(6).
[50] *See Multi Ag Media LLC v. USDA*, 515 F.3d 1224, 1229 (D.C. Cir. 2008).
[51] *See NARA v. Favish*, 541 U.S. 157, 172 (2004)
[52] *Id.*
[53] *U.S. Dept. of State v. Washington Post Co.*, 456 U.S. 595 at 602 (1982).

criminal history, medical history, and social security number.[54] This information is generally given significant protection and, unless a countervailing FOIA public interest in disclosure is shown.[55]

- Outside Individuals Who Contact the Government

Courts have also protected the privacy of outside individuals who contact the government. In *Prudential Locations LLC v. HUD*, No-09-16995, 2013 WL 3339618 (9th Cir. Oct. 9, 2013), the Court of Appeals for the Ninth Circuit considered whether to disclose the names of individuals who sent emails to an agency alleging that a business had violated a federal statute. The Court held that the individuals who contacted the agency "could easily be adversely affected if their identities became known."[56] The court also noted that the authors were vulnerable "to retaliation such as loss of employment or loss of business" and "the possibility of a civil lawsuit," and that there was a "significant risk of harassment, retaliation, stigma, or embarrassment of the authors if their identities [were] revealed."[57] Other courts have taken a similar stance, finding that individuals who write to the government expressing personal opinions generally have some expectation of confidentiality, and their identities, but not necessarily the substance of their letters, ordinarily have been withheld.[58]

However, Courts have often held that names of FOIA requesters[59] and individuals who comment on proposed agency rules should be released.[60]

- Government Employees

Civilian federal employees who are not involved in law enforcement or sensitive occupations generally have no expectation of privacy regarding their names, titles, grades, salaries, and duty

[54] *See e.g. id.; Associated Press v. DOJ*, 549 F.3d 62 at 65 ("Personal information, including a citizen's name, address, and criminal history, has been found to implicate a privacy interest cognizable under the FOIA exemptions.")
[55] *See Id.*
[56] *Id.* at *7.
[57] *Id.*
[58] *See, e.g., Lakin Law Firm, P.C. v. FTC*, 352 F.3d 1122, 1125 (7th Cir. 2003) (finding that the "core purposes" of the FOIA would not be served by the release of the names and addresses of persons who complained to the FTC about "cramming"); *Strout v. U.S. Parole Comm'n*, 40 F.3d 136, 139 (6th Cir. 1994) (articulating public policy against disclosure of names and addresses of people who write Parole Commission opposing convict's parole); *Carter, Fullerton & Hayes LLC v. FTC*, 520 F. Supp. 2d 134, 145 n.4 (D.D.C. 2007) ("Consumers making complaints with the FTC have an expectation that it will protect their personal information."); *Kidd v. DOJ*, 362 F. Supp. 2d 291, 297 (D.D.C. 2005) (protecting names and addresses of constituents in letters written to their congressman); *Voinche v. FBI*, 940 F. Supp. 323, 329-30 (D.D.C. 1996) ("There is no reason to believe that the public will obtain a better understanding of the workings of various agencies by learning the identities of . . . private citizens who wrote to government officials . . . ."), aff'd per curiam, No. 96-5304, 1997 WL 411685 (D.C. Cir. June 19, 1997).
[59] *Agee v. CIA*, 1 Gov't Disclosure Serv. (P-H) ¶ 80,213 at 80,532 (D.D.C. Jul. 23, 1980) ("FOIA requesters . . . have no general expectation that their names will be kept private.")
[60] *Alliance for the Wild Rockies v. Dep't of the Interior*, 53 F. Supp. 2d 32, 36-37 (D.D.C. 1999) (concluding that commenters to proposed rulemaking could have little expectation of privacy when rulemaking notice stated that complete file would be publicly available).

stations as employees[61] or regarding the parts of their successful employment applications that show their qualifications for their positions.[62] However, those employees have a protectable privacy interest in purely personal details that do not shed light on agency functions. The U.S. Supreme Court has recognized the sensitivity of employee's home addresses, in particular, finding that "[d]isclosure of the addresses would not appreciably further the citizens' right to be informed about what their Government is up to and, indeed, would reveal little or nothing about the employing agencies or their activities."[63] Other courts have also protected private contact information of government employees, including signatures, personal phone numbers, personal email addresses, dates of birth, social security numbers, insurance and retirement information, and marital status.[64] Courts generally have recognized the sensitivity of information contained in personnel-related files and have accorded protection to the personal details of a federal employee's service.[65] Generally, federal employees have a privacy interest in their job performance evaluations, even if the evaluations are favorable.[66] Information related to misconduct and mistakes, though, may be released if public interest justifies its release, particularly if the officials involved are high level officials.[67]

---

[61] *See* OPM Regulation, 5 C.F.R. § 293.311 (2011) (specifying that certain information contained in federal employee personnel files is generally available to public); see also FLRA v. U.S. Dep't of Commerce, 962 F.2d 1055, 1059-61 (D.C. Cir. 1992) (noting that performance awards "have traditionally been subject to disclosure"); Core v. USPS, 730 F.2d 946, 948 (4th Cir. 1984) (finding no substantial invasion of privacy in information identifying successful federal job applicants).

[62] *See Knittel v. IRS*, No. 07-1213, 2009 WL 2163619, at *6 (W.D. Tenn. July 20, 2009) (holding that agency is incorrect in its assertion that it is only required to disclose information about employees specifically listed in OPM's regulation, as categories mentioned there are "not meant to be exhaustive"); *Cowdery, Ecker & Murphy, LLC v. Dep't of Interior*, 511 F. Supp. 2d 215, 219 (D. Conn. 2007) ("Because exemption 6 seeks to protect government employees from unwarranted invasions of privacy, it makes sense that FOIA should protect an employee's personal information, but not information related to job function.")

[63] *DOD v. FLRA*, 510 U.S. 487, 500 (1994).

[64] *Pub. Emps. for Envtl. Resp. v. U.S. Sec. Int'l Boundary & Water Comm'n*, 839 F. Supp. 2d 304, 323-24 (D.D.C. 2012) (protecting private contact information of emergency personnel whose names appear in emergency action plans); *Wilson v. United States Air Force*, No. 08-324, 2009 WL 4782120, at *4 (E.D. Ky. Dec. 9, 2009) (finding that signatures, personal phone numbers, personal email addresses, and government email addresses were properly redacted); *Kidd v. DOJ*, 362 F. Supp. 2d 291, 296-97 (D.D.C. 2005) (home telephone number); *Barvick v. Cisneros*, 941 F. Supp. 1015, 1020 (D. Kan. 1996) (personal information such as home addresses and telephone numbers, social security numbers, dates of birth, insurance and retirement information, reasons for leaving prior employment, and performance appraisals); *Stabasefski v. United States*, 919 F. Supp. 1570, 1575 (M.D. Ga. 1996) (names of FAA employees who received Hurricane Andrew assistance payments); *Plain Dealer Publ'g Co. v. U.S. Dep't of Labor*, 471 F. Supp. 1023, 1028-30 (D.D.C. 1979) (medical, personnel, and related documents of employees filing claims under Federal Employees Compensation Act); *Info. Acquisition Corp. v. DOJ*, 444 F. Supp. 458, 463-64 (D.D.C. 1978) ("core" personal information such as marital status and college grades).

[65] *See*, e.g., *Ripskis v. HUD*, 746 F.2d 1, 3-4 (D.C. Cir. 1984) (names and identifying data contained on evaluation forms of HUD employees who received outstanding performance ratings); *Ferrigno v. DHS*, No. 09-5878, 2011 WL 1345168, at *8 (S.D.N.Y. Mar. 29, 2011) (determining that "the Supervisor, the Investigator, and the interviewees whose statements are recorded in the memoranda at issue all have a more than de minimus privacy interest in these memoranda, as being identified as part of Plaintiff's [employment-related harassment] complaint could subject them to embarrassment and harassment").

[66] *Id.*

[67] *See*, e.g., *CASA de Maryland, Inc. v. DHS*, 409 F. App'x 697 (4th Cir. 2011) (per curiam) (affirming district court's decision ordering disclosure of names contained in an internal investigation report authored by DHS's Office of Professional Responsibility in light of evidence produced by plaintiff indicating that agency impropriety might have occurred).

- Distinction Between Government Employees and the Public

Notably there appears to be no distinction under FOIA for government employees vs. members of the public. Both qualify for personal privacy protection under FOIA's exemptions. The only distinction is that sometimes the FOIA public interest in disclosure of information about government employees may be higher, which could tip the balance in favor of disclosure.[68]

- Practical Obscurity

The FOIA's broad conception of privacy also encompasses the doctrines of "practical obscurity." In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989), the Supreme Court found a strong privacy interest in the nondisclosure of records of a private citizen's criminal history, despite the fact that "the information may have been at one time public," because it had "over time become 'practically obscure.'"

Similarly, just because a piece of information could be found elsewhere, such as through a private commercial background check or a search of individual courthouse files, that doesn't necessarily mean it is ineligible for protection under FOIA's privacy exemptions. As the Supreme Court held, individuals can have a cognizable privacy interest in identifying information "that might be found after a diligent search of courthouse files, county archives, [. . .] local police stations," and other publicly available sources of information, but otherwise is not readily available to the public.[69] The Court noted that if such items of information actually "were 'freely available' there would be no need to invoke the FOIA to obtain access to" them.[70] The Supreme Court has specifically applied this to federal employee's home addresses even though they "often are publicly available through sources such as telephone directories and voter registration lists."[71]

Section III Personally Identifiable Information Under State Public Records Laws

In order to keep this research project manageable, for the purposes of this section of the report, the Office has limited its research to exemptions that deal with personal contact information, a smaller subset of PII. Public records exemptions related to personal contact information for all states besides Oregon, as well as the District of Columbia (which maintains its own public records law for local authorities) were surveyed. Generally, all jurisdictions surveyed exempt at least some records containing personal contact information from disclosure, often from the same categories as used in Oregon, although the manner in which it is done varies across jurisdictions.

Oregon's public records law contains numerous exemptions, with many encompassing personal contact information. Twenty-two personal contact information exemptions are currently under review by the Sunshine Committee. This survey has adopted the same definition of personal contact information as used by the Sunshine Committee: information that includes an individual's residential and mailing address(es), personal email address(es) and personal

[68] *Stern v. FBI*, 737 F.2d 84 (D.C. Cir. 1984).
[69] *Id.* at 764.
[70] *Id.*
[71] *DOD v. FLRA*, 510 U.S. 487, 500 (1994).

telephone number(s).[72] These exemptions, both in Oregon and other jurisdictions, often incorporate other types of related PII as well, such as social security numbers and dates of birth.

The personal contact information exemptions identified in other jurisdictions' public records statutes were compared with the exemptions under review by the Sunshine Committee, and the same or similar exemptions were noted.[73] To organize the copious amount of information derived from the comparison of exemptions, this survey groups the twenty two Oregon exemptions below based on the frequency with which their comparable exemptions occur in other jurisdictions, accompanied in some instances with commentary noting the way the information is exempted elsewhere[74]:

- Commonly exempted by other jurisdictions

ORS 192.345(29) The electronic mail address of a student who attends a state institution of higher education listed in ORS 352.002 or Oregon Health and Science University.

Commentary for ORS 192.345(29): Other jurisdictions frequently exempt education records in their entirety, or the PII in the records, or the PII in the records only if disclosure would lead to the identification of an individual in a public school or that represents an unlawful invasion of privacy. For some jurisdictions, this is done only at the primary or higher education level. In addition, while some jurisdictions specify exempt personal contact information to include or only be personal email addresses, others vary and may include categories of personal contact information other than email addresses or merely state that information akin to that of a "personal nature" is exempt.

ORS 192.355(12) Employee and retiree address, telephone number and other nonfinancial membership records and employee financial records maintained by the Public Employees Retirement System pursuant to ORS chapters 238 and 238A.

Commentary for ORS 192.355(12): Commonly exempted to the extent that other jurisdictions specifically refer to current employee, not retirees. However, there is significant variation in other jurisdictions from a total ban on disclosing this information, to a ban only on disclosing PII or PII if it is an unlawful invasion of privacy, to a total ban on disclosure, but only for law enforcement and/or public safety officials. Furthermore, in some jurisdictions, an employee must affirmatively communicate with their employer and/or government agencies in possession of

[72] April 30, 2018 memorandum from Michael Kron to Oregon Sunshine Committee Members entitled "Exemptions to be Reviewed at May 16, 2018 Meeting"; https://www.doj.state.or.us/wp-content/uploads/2018/05/OSC_2018-05-16_Exemption_Summaries.pdf.

[73] Although additional public records exemptions may be found in other jurisdictions' statutes besides their public records law, as well as in case law, examination of these sources was beyond the scope of this survey. Therefore, the occurrence of exemptions comparable to Oregon's may vary nationally at an overall rate different than as noted by this survey.

[74] Certain Oregon personal information exemptions may appear in more one category if they encompass more than one type of exemption.

their information to exclude it from disclosure, either at the outset of their employment or after they are notified that the information has been requested in a public records request.

ORS 192.355(3)	Upon compliance with ORS 192.437, public body employee or volunteer residential addresses, residential telephone numbers, personal cellular telephone numbers, personal electronic mail addresses, driver license numbers, employer-issued identification card numbers, emergency contact information, Social Security numbers, dates of birth and other telephone numbers contained in personnel records maintained by the public body that is the employer or the recipient of volunteer services.

Commentary for ORS 192.355(3): Commonly exempted for public employees only, not volunteers.

ORS 403.135(2)	Automatic telephone number identifications received by public safety answering points are confidential and are not subject to public disclosure unless and until an official report is written by the public or private safety agency and that agency does not withhold the telephone number under ORS 192.311 to 192.478 or other state and federal laws. The official report of a public safety answering point may not include nonpublished or nonlisted telephone numbers. The official report of a public or private safety agency may not include nonpublished or nonlisted telephone numbers. Nonpublished or nonlisted telephone numbers are not otherwise subject to public disclosure without the permission of the subscriber.
ORS 403.135(5)(5)	Subscriber information acquired by a 9-1-1 jurisdiction for the purpose of providing emergency communications services under ORS 403.105 to 403.250 is not subject to public disclosure and may not be used by other public agencies except: (a) To respond to an emergency call; (b) To respond to an emergency situation that involves the risk of death or serious physical harm to an individual, as provided in ORS 403.132; or (c) To notify the public of an emergency by utilizing an automated notification system if a provider has provided subscriber information to the 9-1-1 jurisdiction or emergency services provider.
ORS 350.278	Social security numbers of college students.
ORS 350.280	Social security number of community college students.

Commentary for ORS 350.278 and 350.280: Although some exemptions for the disclosure of the personal contact information in records for college students may be common in other jurisdictions, similar to the commentary for ORS 192.345(29), above, the form of the exemption varies; i.e., it may not be specific to a student's social security number, but more generally to the entire file, PII in the file, or PII in a file if disclosure is an unwarranted invasion of privacy.

ORS 192.355(23)	Contact information of library patrons.

ORS 192.355(28) Personal and contact information of public utility customers.

- Sometimes exempted by other jurisdictions

ORS 192.345(25) The home address, professional address and telephone number of a person who has or who is interested in donating money or property to the Oregon University System.

Commentary for ORS 192.345(25): Similar exemptions exist for donors in other jurisdictions for higher education institutions specifically or government agencies generally.

ORS 676.405(2)(2) Notwithstanding ORS 192.311 to 192.478, a health professional regulatory board may, at its discretion, release or withhold the personal electronic mail address, home address and personal telephone number for a person licensed, registered or certified by the board. If the personal electronic mail address, home address or personal telephone number is requested for a public health or state health planning purpose, the board shall release the information

- Infrequently exempted by other jurisdictions

ORS 192.355(12) Employee and retiree address, telephone number and other nonfinancial membership records and employee financial records maintained by the Public Employees Retirement System pursuant to ORS chapters 238 and 238A.

Commentary for ORS 192.355(12): To the extent that other jurisdictions' specifically refer to the same or similar information of a retiree or former public employee.

ORS 192.355(29) A record of the street and number of an employee's address submitted to a special district to obtain assistance in promoting an alternative to single occupant motor vehicle transportation.

ORS192.355(40)(a) Electronic mail addresses in the possession or custody of an agency or subdivision of the executive department, as defined in ORS 174.112, a local government or local service district, as defined in ORS 174.116, or a special government body, as defined in ORS 174.117. (b) This subsection does not apply to electronic mail addresses assigned by a public body to public employees for use by the employees in the ordinary course of their employment.

Commentary for ORS 192.355(40(a): Personal contact information is frequently exempted in some manner by most jurisdictions, but few specifically protect all email addresses in all instances.

ORS 192.365 (1) Upon compliance with ORS 192.363, a public body that is the custodian of or is otherwise in possession of the following information pertaining to a home care worker as defined in ORS 410.600, an operator of a child care facility as defined in ORS 329A.250, an exempt family child care provider as defined in ORS 329A.430 or an operator of an adult foster home as defined in ORS 443.705 shall disclose that information in response to a request to inspect public records under ORS 192.311 to 192.478: (a) Residential address and telephone numbers; (b) Personal electronic mail addresses and personal cellular telephone numbers; (c) Social Security numbers and employer-issued identification card numbers; and (d) Emergency contact information. (2) Subsection (1) of this section does not apply to the Judicial Department or the Department of Transportation or to any records in the custody of the Judicial Department or the Department of Transportation.

ORS 802.177 Personal information contained in motor vehicle records.

ORS 802.181 Redisclosure of information contained in motor vehicle records.

ORS 802.195 Social security numbers in motor vehicle records.

- Never exempted by other jurisdictions

ORS 165.673 No law enforcement agency shall disclose lists of telephone numbers produced by a pen register or trap and trace device except in the performance of a law enforcement function or as otherwise provided by law or order of a court.

ORS 192.355(3) Upon compliance with ORS 192.437, public body employee or volunteer residential addresses, residential telephone numbers, personal cellular telephone numbers, personal electronic mail addresses, driver license numbers, employer-issued identification card numbers, emergency contact information, Social Security numbers, dates of birth and other telephone numbers contained in personnel records maintained by the public body that is the employer or the recipient of volunteer services.

Commentary for ORS 192.355(3): Never exempted to the extent that other jurisdictions specifically refer to volunteer, not public body employee.

ORS 646.574(3)(3) Information about a party (to a do-not-call list) is confidential. The Attorney General may not disclose information about a party.

ORS 107.840 Social security numbers of parties to divorce actions in court records.

ORS 192.345(28) Social security numbers of parties to divorce actions in court records.

ORS 432.360 Social security numbers of parties to divorce actions in county records.

Section IV Selective Waiver of Conditional Exemptions

Some public records in Oregon are conditionally exempt from disclosure, and may be disclosed upon satisfying a balancing test that weighs a recognized governmental or private interest in confidentiality against the public interest in disclosure. Under consideration by the Sunshine Committee is whether a public body may selectively waive an exemption and disclose a conditionally exempt record to an individual requestor to use for a specific purpose that satisfies such a test, while restricting the requestor from using the record in any other way. Although this is not a settled matter in Oregon law, there is currently no prohibition that prevents a public body from waiving an exemption and disclosing a conditionally exempt record in this manner. Other states surveyed impose various limitations on disclosure.

Many of the over 550 exemptions to disclosure of a public record are contained in ORS sections 192.345 and 192.355. All of the exemptions in ORS 192.345 and several in ORS 192.355 are conditional, and require satisfaction of a balancing test before they may be waived. A public body's determination to waive an exemption under the balancing tests in these sections is fact-specific and each request must be considered on a case-by-case basis. Therefore, while some requests may be granted, others will not be, and a public body may disclose a record to a successful requestor while preserving the exemption as to the public generally. Absent a prohibition in Oregon's public record law, it follows that a public body may also selectively waive an exemption only for the stated purpose in the request that satisfied the balancing test, while restricting the requestor from using the record for any other purpose that was not considered and/or did not satisfy the balancing test. In doing so, the exemption could be preserved by the public body except for the basis under which the waiver was granted.

Although this issue has not been the subject of legislation or extensive litigation, it has been the opinion of the Oregon Attorney General that provision of conditionally exempt public records to a specific requestor does not create a general public waiver of an exemption as to that record:

> "A public body occasionally may wish to disclose an exempt public record to a specific private individual, but not to the public at large. The question then arises whether, by selectively disclosing an exempt record, the public body loses its discretionary power to claim the exemption as to other requesters. We have concluded that, under certain circumstances, the public body still retains that power, stating: '[W]here limited disclosure of a public record does not thwart the policy supporting the exemption, the public body does not thereby waive its prerogative not to disclose the record to others.'"[75]

Determining whether disclosure would thwart the policy (of maintaining a recognized governmental or private interest in confidentially) supporting an exemption occurs when undertaking the balancing test contained within that exemption. Although the burden of proof may reside with either the public body or requestor depending on which exemption is at issue,

[75] Attorney General's Public Records and Meetings Manual, November 2014 edition, p. 119, citing to Letter of Advice dated March 29, 1988, to W.T. Lemman, Executive Vice Chancellor.

any waiver would still occur only upon satisfaction of the test and only for the specific request under consideration. That is why the test must be fact driven, and by its very nature include a review of the purpose and purported usage of the record subject to the request for disclosure. This variability as to waiving an exemption was recognized by the Oregon Court of Appeals in *Oregonian Publishing Company v. Portland School District No. 1J*, 152 Or.App. 135, 142 (1998), in which it held that "there is no blanket principle that applies to waiver under the Oregon public records inspection law."

Therefore, it is clear that disclosure of a conditionally exempt record in Oregon can be selective, with different outcomes for the same record depending on the requestor and the nature of the request. Moreover, the exemption always resides with the public body, and is retained even when a waiver is granted in a particular instance.[76] As such, disclosure of a conditionally exempt public record as to one is not disclosure as to all, i.e., the public generally, and the exemption remains with the public body, even after a waiver is granted.

There is currently no provision in Oregon's public records law that prohibits a public body from going a step further to ensure that conditionally exempt records are used in the manner that led to a waiver by restricting usage of the disclosed record for anything other than what was authorized by the waiver. A law similar to this ability to restrict disclosure can be found in Georgia's Open Records Act, section 50-18-72(20)(C), which states:

> "Records and information disseminated pursuant to this paragraph maybe used only by the authorized recipient and only for the authorized purpose. Any person who obtains records or information pursuant to the provisions of this paragraph and knowingly and willfully discloses, distributes, or sells such records or information to an unauthorized recipient or for an unauthorized purpose shall be guilty of a misdemeanor of a high and aggravated nature and upon conviction thereof shall be punished as provided in Code Section 17-10-4. Any person injured thereby shall have a cause of action for invasion of privacy."

The records and information covered by this paragraph are found in section 50-18-72(20)(A) and are:

> "Records that reveal an individual's social security number, mother's birth name, credit card information, debit card information, bank account information, account number, utility account number, password used to access his or her account, financial OPEN RECORDS ACT 2012 -11- data or information, insurance or medical information in all records, unlisted telephone number if so designated in a public record, personal e-mail address or cellular telephone number, day and month of birth, and information regarding public utility, television, Internet, or telephone accounts held by private customers, provided

[76] *See Smith v. Coulombe*, 2013 WL 428363 *14 (D.Or. Feb. 4, 2013) ("The Court notes, in further support of the finding that Oregon privacy laws do not preclude production of the Second Stoelk Report and that production of the report would not subject Defendants to potential civil liability from employees whose information is included in the report, that any confidential status of the report belongs to the City of Hermiston and not to any employee, and that the City can waive its authority to withhold such records," citing to *Oregonian Publishing*, supra.)

> that nonitemized bills showing amounts owed and amounts paid shall be available."

These records are conditionally exempt to the extent that the information contained in the records will not be redacted upon request "if the person or entity requesting such records requests such information in a writing signed under oath by such person or a person legally authorized to represent such entity which states that such person or entity is gathering information as a representative of a news media organization for use in connection with news gathering and reporting; and provided, further, that such access shall be limited to social security numbers and day and month of birth . . ."[77]

Other illustrative examples of the limitations on usage of records that may otherwise be disclosed is the restriction on commercial usage found in many states' public records law, such as Kansas [K.S.A. 45-221(c)], Kentucky [KRS 61.874(5)] and South Carolina [S.C. Code Ann. 30-450(B), 30-4-160]. These laws limit or restrict the resale or distribution of public records for commercial purposes, or for commercial purposes other than what was intended at the time of request. For instance, under Arizona's Revised Statutes (ARS) 39-121-03:

> "(C) A person who obtains a public record for a commercial purpose without indicating the commercial purpose or who obtains a public record for a noncommercial purpose and uses or knowingly allows the use of such public record for a commercial purpose or who obtains a public record for a commercial purpose and uses or knowingly allows the use of such public record for a different commercial purpose or who obtains a public record from anyone other than the custodian of such records and uses it for a commercial purpose shall in addition to other penalties be liable to the state or the political subdivision from which the public record was obtained for damages in the amount of three times the amount which would have been charged for the public record had the commercial purpose been stated plus costs and reasonable attorney fees or shall be liable to the state or the political subdivision for the amount of three times the actual damages if it can be shown that the public record would not have been provided had the commercial purpose of actual use been stated at the time of obtaining the records.
>
> (D) For the purposes of this section, 'commercial purpose' means the use of a public record for the purpose of sale or resale or for the purpose of producing a document containing all or part of the copy, printout or photograph for sale or the obtaining of names and addresses from public records for the purpose of solicitation or the sale of names and addresses to another for the purpose of solicitation or for any purpose in which the purchaser can reasonably anticipate the receipt of monetary gain from the direct or indirect use of the public record. Commercial purpose does not mean the use of a public record as evidence or as research for evidence in an action in any judicial or quasi-judicial body."

In sum, for public records that are conditionally exempt but disclosed by a public body under a selective waiver, there is currently no prohibition in Oregon law preventing provision of the

[77] Georgia Law section 50-18-72(20)(A).

records for the express purpose for which the waiver is granted, while restricting further usage or distribution of the records. Other states public records laws contain limitations on disclosure in variable circumstances that might be of interest to the Sunshine Committee.

Section V Conclusion

In conclusion, the disclosure of PII poses significant risks, including the risk of identity theft, doxing, and swatting, which should be closely considered by the Committee as it proceeds. Victims of identity theft often face long and costly battles to recover their credit, finances, and security. Victims of swatting and doxing face very real and lasting threats of violence and reprisal. Identity theft, doxing, and swatting are all increasingly common.

In light of these risks, other jurisdictions have taken a cautious approach to release of PII, particularly personal contact information. Many jurisdictions limit the disclosure of personal addresses, personal email addresses, personal phone numbers, and other related PII. While some states do draw distinctions between the privacy of government employees and the privacy of members of the public, the federal government does not.

One possible path to balance these privacy interest with the public interest in disclosure is to grant selective waiver of exemptions – to release information to only a particular requester for a particular purpose. Some jurisdictions have taken this approach.

The Office of the Public Records Advocate thanks the Sunshine Committee for its time and attention to this important issue and looks forward to reading the Committee's conclusions. Questions about this report can be directed to Ginger McCall, Public Records Advocate, 503-378-5228, ginger.mccall@oregon.gov.