

WHEN WHISPERS ENTER THE CLOUD: EVALUATING
TECHNOLOGY TO PREVENT AND REPORT SEXUAL ASSAULT

Heidi Liu*

TABLE OF CONTENTS

I. INTRODUCTION.....	939
II. TECHNOLOGIES FOR SEXUAL MISCONDUCT PREVENTION.....	942
A. Prevention.....	942
B. Response.....	944
C. Prediction.....	946
III. EVALUATION OF EXISTING APPLICATIONS.....	948
A. Privacy.....	949
1. Notice and Choice.....	949
2. Access.....	953
3. Security.....	954
4. Incentives to Adopt Technological Interventions.....	955
B. Increasing Take-Up.....	956
1. Design.....	958
2. Cultural Stereotypes of Harassment/Assault.....	959
3. Standards for Reporting.....	960
IV. CONCLUSION.....	961

I. INTRODUCTION

On October 11, 2017, a Google spreadsheet that collected allegations of assault, harassment, and “creepy behavior” of male coworkers began circulating among female employees in the media industry.¹ Viewers had the ability to add their own accusations to the spreadsheet, which had columns for an employee’s name, media affiliation, and accused behavior.² While the list was initially privately distributed among media industry employees,³ the link to the sheet could be

* Ph.D. student in public policy, Harvard University; J.D. 2017, Harvard Law School; A.B. 2011, Harvard College.

1. Doree Shafrir, *What To Do With “Shitty Media Men”?*, BUZZFEED (Oct. 12, 2017, 12:48 AM), <https://www.buzzfeed.com/doree/what-to-do-with-shitty-media-men> [<https://perma.cc/7QHQ-5P6S>].

2. Jia Tolentino, *The Whisper Network After Harvey Weinstein and “Shitty Media Men,”* NEW YORKER (Oct. 14, 2017), <https://www.newyorker.com/news/news-desk/the-whisper-network-after-harvey-weinstein-and-shitty-media-men> [<https://perma.cc/84CL-CAFD>]; Shafrir, *supra* note 1.

3. Tolentino, *supra* note 2.

accessed by anyone.⁴ By early Thursday morning — less than 24 hours later — a BuzzFeed article reported on the existence of the list, which turned private,⁵ and a plethora of thinkpieces began debating the spreadsheet’s merits.⁶ Journalists talked about their experiences of seeing colleagues on the so-called “Shitty Media Men” list,⁷ while a right-wing pundit threatened to publish names from the list.⁸

In describing her experience with the spreadsheet in *The New Yorker*, Jia Tolentino categorizes the Shitty Media Men list as an example of a “whisper network,” that is, “the unofficial information channel that women use to warn each other about men whose sexual behavior falls on the spectrum from creepy to criminal.”⁹ There are whisper networks in many contexts;¹⁰ for example, when colleagues warn each other about a boss’s touchy behavior.¹¹

Only recently has technology been used to collate allegations or to prevent sexual assault. The distribution and subsequent publicity of the Shitty Media Men list can help illustrate the legal difficulties that arise from using technology to do so. First, one fear is that data collection of allegations could lead to *false* allegations.¹² That is, there is a tradeoff between the ease with which someone can make an allegation of assault and the likelihood of a false allegation. Falsely accused individuals may face undeserved stigma, and the first instance of a false allegation could undermine credibility of the entire spreadsheet.

How accusations are sourced is a related concern. A false record is difficult to correct when it is not clear where that record began.¹³ In the Shitty Media Men list, anyone could post an allegation — whether true or false.¹⁴ Even if a false accusation were deleted, the spreadsheet

4. *Id.*

5. *Id.*

6. See generally *id.*; see also Michael Calderone & Jason Schwartz, *Blogger Amends Vow To Publish List of “Shitty Media Men,”* POLITICO (Oct. 25, 2017, 9:11 PM), <https://www.politico.com/story/2017/10/25/cernovich-media-harass-list-244180> [https://perma.cc/ZS6J-EWAC].

7. See Tolentino, *supra* note 2; see also Katy Waldman, *This Week, It Was Particularly Rough To Be a Woman*, SLATE (Oct. 13, 2017, 7:29 PM), http://www.slate.com/blogs/xx_factor/2017/10/13/in_the_wake_of_the_harvey_weinstein_scandal_it_feel_rough_to_be_a_woman.html (last visited May 5, 2018).

8. Calderone & Schwartz, *supra* note 6.

9. Tolentino, *supra* note 2.

10. See Summer Meza, *What is a Whisper Network? How Women Are Taking Down Bad Men in the #MeToo Age*, NEWSWEEK (Nov. 22, 2017, 1:51 PM), <http://www.newsweek.com/what-whisper-network-sexual-misconduct-allegations-719009> [https://perma.cc/P6DP-QXGC].

11. See Tolentino, *supra* note 2; see also Meza, *supra* note 10.

12. See Moira Donegan, *I Started the Media Men List*, THE CUT (Jan. 10, 2018, 10:12 PM), <https://www.thecut.com/2018/01/moira-donegan-i-started-the-media-men-list.html> [https://perma.cc/8N3X-VU5R].

13. See generally *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

14. See Tolentino, *supra* note 2; see also Shafir, *supra* note 1; Donegan, *supra* note 12.

history would record changes to the sheet,¹⁵ which would deter accurately accused individuals from deleting the relevant accusation.

As Tolentino points out, “[t]he whisper network is an informal but relatively orderly reporting method, regulated by the direct accountability of a social ecosystem: if I give you false information, then my credibility and relationships will suffer.”¹⁶ At face value, an anonymized, publicly viewable spreadsheet may appear to lack direct accountability. However, that the spreadsheet was intended for and privately distributed among media employees lent it initial credibility to newcomers to the industry. By January 2018, the originator of the Shitty Media Men list, Moira Donegan, revealed herself in an article on *New York Magazine’s The Cut*.¹⁷ As she noted, “to make [the list] I relied on backchannels and friendships that I only developed after having been in media for some time . . . I didn’t have this information when I was 22, interning”¹⁸

At the same time, a sexual assault survivor has privacy concerns of her own. The process of reporting an experience publicly can be re-traumatizing, with significant consequences even when reporting a true claim.¹⁹ Donegan, for example, feared being outed when a Harper’s Monthly fact checker called Donegan to ask if she was indeed the originator of the spreadsheet.²⁰ Donegan’s precautions in maintaining anonymity appear to have failed.

While technology can enable anonymity and information dissemination, these features should be reckoned with when discussing a platform that may generate accusations of criminal behavior or may lead to further intimidation of survivors. When someone is accused of sexual assault in a criminal adjudication, the prosecution must show that the defendant is guilty beyond a reasonable doubt.²¹ In a campus setting, until earlier this fall, the relevant standard for disciplinary action against a student accused of sexual harassment was the “preponderance of the evidence” standard.²² At present, universities may choose between maintaining the preponderance standard or using the more demanding standard of “clear and convincing evidence” in their adjudications.²³ Opponents of the Shitty Media Men list claim that

15. See *What’s Changed in a File*, GOOGLE, <https://support.google.com/docs/answer/190843> [<https://perma.cc/62BH-DDGE>].

16. *Id.*

17. Donegan, *supra* note 12.

18. *Id.*

19. See Eliza Gray, *Why Victims of Rape Don’t Report to the Police*, TIME (June 23, 2014), <http://time.com/2905637/campus-rape-assault-prosecution/> [<http://perma.cc/4PQY-ZMQH>].

20. Donegan, *supra* note 12.

21. See, e.g., Julie Novkov, *Equality, Process and Campus Sexual Assault*, 75 MD. L. REV. 590, 598 (2016).

22. See DEP’T. OF EDUC., DEAR COLLEAGUE LETTER 10–11 (2011).

23. See DEP’T. OF EDUC., Q&A ON CAMPUS SEXUAL MISCONDUCT 5 (2017).

men are being accused of actions without regard to due process,²⁴ while others argue that it is precisely because few accusations are reported to authorities that a spreadsheet or other mechanism is necessary.²⁵

In the seven years since the Department of Education laid out standards for university investigations of sexual assault in its 2011 Dear Colleague letter,²⁶ commentators have argued that harassment prevention is “now an exploding industry with . . . all kinds of crash courses on how to get and give consent.”²⁷ This Note considers these legal issues around the use of technology for predicting and reporting sexual misconduct. Part II provides a brief overview of the existing technologies on the market and evaluates their benefits and drawbacks. Part III evaluates these technologies with regard to both privacy concerns and user experience, offering specific suggestions for design.

II. TECHNOLOGIES FOR SEXUAL MISCONDUCT PREVENTION

Different technologies use different points of intervention that occur prior to, during, or after misconduct. This Part describes existing examples of interventions chronologically and evaluates whether their features and purposes can successfully work towards reducing sexual assault generally.

A. Prevention

One set of existing smartphone apps seeks to prevent an initial assault from occurring, primarily by making it easier for a potential target to ask for help. For instance, during a government hackathon,²⁸ a team of sexual assault survivors developed Circle of 6, a smartphone app that allows users to create a circle of friends who they can mass

24. See, e.g., Katie Roiphe, *The Other Whisper Network*, HARPER’S (Mar. 2018), <https://harpers.org/archive/2018/03/the-other-whisper-network-2/2/> [https://perma.cc/4W WX-FBG7].

25. See, e.g., Casey Quinlan, *The Shitty Media Men List and Other Ways Women Can Report Misconduct*, THE GUARDIAN (Jan. 13, 2018, 9:59 AM), <https://www.theguardian.com/world/2018/jan/13/sexual-harassment-shitty-media-men-list-examples> [https://perma.cc/XXL6-SKQ9].

26. See generally DEP’T. OF EDUC., *supra* note 22.

27. See Tovia Smith, *Curbing Sexual Assault Becomes Big Business on Campus*, NPR (Aug. 12, 2015, 4:42 PM), <https://www.npr.org/2015/08/12/430378518/curbing-sexual-assault-becomes-big-business-on-campus> (last visited May 5, 2018).

28. See *Apps Against Abuse Hackathon*, DEVPOST, <https://appsagainstabuse.devpost.com/> [https://perma.cc/EDV7-SX68].

text with their location when they feel unsafe.²⁹ That is, the app allows you to contact all six friends with one button and prepopulated texts, increasing the likelihood that at least one will respond immediately and reducing the time it takes to ask for help. Other apps, such as RaveGuardian, allow users to send alarms or GPS signaling to individual contacts,³⁰ particularly when the user is walking alone,³¹ and to record an incident.³² Accordingly, these apps are also used for other purposes, i.e., for indicating school emergencies³³ or to record bullying in schools.³⁴ While smartphones typically have the capability to send their location to others,³⁵ these apps reduce the effort it takes to do so while providing specific context.

A second set of smartphone apps allow participants to record their alcohol levels or a verbal indication of consent.³⁶ The theory behind the development of these apps is that both a potential accuser or defendant can benefit from video or audio proof supporting an allegation that an encounter was consensual or non-consensual.³⁷ We-Consent, for example, is an app where each party to a sexual encounter records themselves on video giving verbal consent.³⁸ Developed by an institu-

29. See Juana Summers, *Smartphone Apps Help To Battle Campus Sexual Assaults*, NPR (Aug. 13, 2014, 4:32 AM), <https://www.npr.org/2014/08/13/339888170/smartphone-apps-help-to-battle-campus-sexual-assaults> (last visited May 5, 2018).

30. RAVEGUARDIAN, <http://www.raveguardian.com/> [https://perma.cc/ME99-XA4V]; see also Lauren Kassien, *5 Apps Fighting Back Against Sexual Assault*, PASTE (Feb. 6, 2015, 9:09 AM), <https://www.pastemagazine.com/articles/2015/02/five-apps-fighting-back-against-sexual-assault.html> [https://perma.cc/JZP8-KYNG].

31. See *Virtual Safety: In Wake of Sex Assaults, 'Buddy' Apps Track Users Walking Alone*, CTVNEWS (Apr. 1, 2016, 10:56 PM), <https://www.ctvnews.ca/sci-tech/virtual-safety-in-wake-of-sex-assaults-buddy-apps-track-users-walking-alone-1.2842547> (last visited May 5, 2018).

32. See Jordana Cepelewicz, *The Apps that Are Changing American Cities*, POLITICO (June 10, 2014), <https://www.politico.com/magazine/story/2014/06/apps-that-are-changing-american-cities-107678> [https://perma.cc/NZN9-U3SA].

33. See Anaya Bhattacharya, *The US Navy is Trying To Deal with its Sexual Assault Problem by Giving Sailors a Reporting App*, QUARTZ (Dec. 9, 2016), <https://qz.com/858321/us-navy-on-duty-sexual-assault-prevention-app/> [https://perma.cc/FTW8-DGRA].

34. See Rebecca Greenfield, *Harassment Hotlines Don't Work. Will Apps?*, BLOOMBERG (June 13, 2017, 5:15 AM), <https://www.bloomberg.com/news/articles/2017-06-13/can-apps-get-victims-to-report-workplace-harassment> [https://perma.cc/7539-662S].

35. See, e.g., Brian Chen, *When You Should (or Shouldn't) Share Your Location Using a Smartphone*, N.Y. TIMES (July 12, 2017), <https://www.nytimes.com/2017/07/12/technology/personaltech/using-location-sharing-apps.html> (last visited May 5, 2018).

36. See Mehak Anwar, *"We-Consent" App Aims To Decrease Sexual Assault and Rape, But Can Apps Really Solve the Problem?*, BUSTLE (July 16, 2015), <https://www.bustle.com/articles/97697-we-consent-app-aims-to-decrease-sexual-assault-and-rape-but-can-apps-really-solve-the-problem> [https://perma.cc/6S9R-UA2A]; Emily Cegielski, *"Yes Means Yes," But New Consent Apps Draw Concern from College Students*, WOMEN IN THE WORLD (July 28, 2015), <https://womenintheworld.com/2015/07/28/yes-means-yes-but-new-consent-apps-draw-concern-from-college-students/> [https://perma.cc/NF7R-XRM8].

37. See Anwar, *supra* note 36.

38. *Id.*

tion called the Institute for the Study of Coherence and Emergence, the app is meant to be used before an encounter.³⁹ A video prompts users to choose “Yes,” “No,” or “Forced Yes.”⁴⁰ “If one party says ‘no’ the video record self-destructs . . . but the response ‘forced yes’ will create a record of the coercion.”⁴¹ The videos are stored on We-Consent’s servers for seven years.⁴²

Good2Go, a similar app, asks first for consent, then for an individual’s self-perceived level of intoxication.⁴³ The options given are “No, Thanks,” “Yes, but . . . we need to talk,” and “I’m Good2Go.”⁴⁴ If the user states that he is “Pretty Wasted,” then the app informs him that he is unable to consent.⁴⁵ The user then passes the phone to his potential partner, who views the level of intoxication and consent of his partner, then presses a button to consent.⁴⁶

Most recently, a Dutch company launched “LegalFling,” an app that sends potential partners information requests including the sexual preferences of the other individual (e.g., condom usage). If both partners accept the other’s request, the contract is recorded on the blockchain.⁴⁷

B. Response

In addition to the whisper network discussed above — which could be categorized as a relatively informal, industry-based networks — harassment may be reported after sexual misconduct occurs through venues occasionally provided by the institution the survivor is associated with, such as their employer or university. Some employers have created anonymous hotlines to report misconduct.⁴⁸ At Google, an email list called “Yes, at Google” provides a venue for employees

39. See WE-CONSENT, <http://we-consent.org/> [<https://perma.cc/YAH3-RZ9S>].

40. See App Store Preview: We-Consent, APPLE, <https://itunes.apple.com/us/app/we-consent/id964520119?mt=8> (last visited May 5, 2018).

41. *Id.*

42. See Anwar, *supra* note 36.

43. See Amanda Hess, *Consensual Sex: There’s an App for That*, SLATE (Sept. 29, 2014, 9:17 AM), http://www.slate.com/blogs/xx_factor/2014/09/29/good2go_a_new_app_for_consenting_to_sex.html (last visited May 5, 2018).

44. *Id.*

45. *See id.*

46. *See id.*

47. See Valentina Zarya, *Is Blockchain the Answer to Sexual Consent?*, FORTUNE (Jan. 16, 2018), <http://fortune.com/2018/01/16/consent-app-me-too/> (last visited May 5, 2018).

48. See Noam Scheiber, *Anonymous Harassment Hotlines Are Hard To Find and Harder To Trust*, N.Y. TIMES (Apr. 21, 2017), <https://www.nytimes.com/2017/04/21/business/media/fox-sexual-harassment-hotline-bill-oreilly.html> (last visited May 5, 2018). The hotline trend is also observed in non-workplace settings: the band Speedy Ortiz provide a hotline when attendees perceive unsafe behavior. See Matthew Strauss, *Speedy Ortiz Open “Help Hotline” for Fans Who Feel Unsafe at Their Shows*, PITCHFORK (Sept. 7, 2015), <https://pitchfork.com/news/61103-speedy-ortiz-open-help-hotline-for-fans-who-feel-unsafe-at-their-shows/> [<https://perma.cc/9FPQ-YV5L>].

to anonymously disseminate incidents of harassment.⁴⁹ Kaiser Permanente uses the StopIt application, which allows individuals to report harassment with multimedia evidence directly to an HR department.⁵⁰ Finally, some universities allow assaults to be reported via smartphone apps.⁵¹

The platform Callisto has been adopted widely.⁵² Callisto, a non-profit whose current clients include universities and the comedy school Upright Citizens Brigade, is an online platform where survivors have three options: “1) create a time-stamped, secure record of sexual assault, 2) report electronically by sending a record to the school, or 3) only notify the school if another student names the same perpetrator.”⁵³ That is, if multiple people report the same person, their records would be jointly sent to the school. Because the record is time-stamped,⁵⁴ officials can see the time between when the misconduct allegedly occurred and when the account was written. Callisto utilizes the concept of “information escrows.”⁵⁵ An “information escrow” is a third-party agent that holds on to the relevant information⁵⁶ and disseminates it when others report similar behavior or the same bad actor to the escrow.⁵⁷ Individuals may not wish to be the first to report problematic behavior,⁵⁸ because of the relatively high costs

49. See Ellen Huet & Mark Bergen, *At Google, an Employee-Run Email List Tracks Harassment and Bias Complaints*, BLOOMBERG (May 23, 2017, 6:00 AM), <https://www.bloomberg.com/news/articles/2017-05-23/at-google-an-employee-run-email-list-tracks-harassment-and-bias-complaints> [<https://perma.cc/CK4P-3JE9>].

50. See Greenfield, *supra* note 32.

51. See Jamie Brensilber, *Students Can Now Anonymously Report Sexual Assaults Through Penn Guardian App*, THE DAILY PENNSYLVANIAN (Apr. 27, 2016, 2:34 AM), <http://www.thedp.com/article/2016/04/student-report-sexual-violence-penn-guardian-app> [<https://perma.cc/NL8W-Q6BY>]; Sarah Rich, *App Helps Victims Report Sexual Assault Anonymously in DC*, GOV. TECH (Aug. 19, 2013), <http://www.govtech.com/health/App-Helps-Victims-Report-Sexual-Assault-Anonymously-in-DC.html> [<https://perma.cc/V8GN-2SE2>] (describing an app modelled after one used in D.C. area universities).

52. See generally *2016-2017 School Year Report*, CALLISTO (2017), available at https://www.projectcallisto.org/Callisto_Year_2_highres.pdf [<https://perma.cc/4XDP-E4SX>]. Its donors include entities such as Google.org, with over \$500,000 reported in funds raised during the first 9 months of 2017.

53. *Id.* at 3. The survivor does not need to decide whether to send the record immediately, and even if her record is not matched, she can choose to send the record at a later point. *Id.* at 5.

54. See *id.* at 3.

55. See generally Ian Ayres & Cait Unkovic, *Information Escrows*, 111 MICH. L. REV. 145 (2012).

56. *Id.* at 150.

57. *Id.* at 148.

58. See Ian Ayres, *Meet Callisto, the Tinder-Like Platform That Aims To Fight Sexual Assault*, WASH. POST (Oct. 9, 2015), https://www.washingtonpost.com/opinions/using-game-theory-technology-to-fight-sexual-assault/2015/10/09/f8ebd44e-6e02-11e5-aa5b-f78a98956699_story.html?utm_term=.aacca49d23e1 [<https://perma.cc/S6CL-U2LH>]. The use of information escrows might extend to contexts outside of sexual harassment, including falsification of research results or in the background check for an employer. See David D. Laitin & Rob Reich, *Trust, Transparency and Replication in Political Science*, 50 POL. SCI.

involved (e.g., more scrutiny);⁵⁹ however, they may wish to do so if there are multiple people experiencing the same thing, either because the individual recognizes that the assailant may otherwise engage in misconduct again, or because their report gains credibility if it is not the only one.⁶⁰

Other reporting apps include the I've-Been-Violated app, developed by the same founders as We-Consent.⁶¹ I've-Been-Violated prompts a survivor to make a time-stamped video where one can speak about the assault.⁶² The survivor can then contact the police or a university office, and they, in turn, can reach out to the app developer to obtain the video.⁶³

Lighthouse, another competitor of Callisto's, allows survivors — as well as witnesses — to report an assault.⁶⁴ According to Lighthouse, once a report is completed, it is “automatically sent to the Title IX coordinator for the student's campus, but Lighthouse can also choose to send it to campus security, the local police department, and/or the regional Office for Civil Rights,”⁶⁵ in contrast with Callisto, which allows users to delay reporting. After the report has been sent, “users and [university] officials can see who has logged in, viewed the report, and so on.”⁶⁶

C. Prediction

Finally, in conjunction with reporting, technology has also been used to attempt to predict patterns of misbehavior. On its fact sheet, Callisto lists “data on victimization and perpetration trends,” as ag-

& POL. 172, 174 (2017); Peter Baumhart, *Social Media and the Job Market: How To Reconcile Applicant Privacy with Employer Needs*, 48 U. MICH. J. L. REFORM 503, 524–25 (2015).

59. See Natasha Singer, *The War on Campus Sexual Assault Goes Digital*, N.Y. TIMES (Nov. 13, 2015), <https://www.nytimes.com/2015/11/15/technology/the-war-on-campus-sexual-assault-goes-digital.html> (last visited May 5, 2018).

60. Olga Khazan, *Can Game Theory Help To Prevent Rape?*, THE ATLANTIC (Sept. 17, 2015), <https://www.theatlantic.com/technology/archive/2015/09/can-game-theory-prevent-rape/405607/> [<https://perma.cc/9XPH-W8F3>]; see also Nora Caplan-Bricker, *Stanford Becomes the Most Prominent School Yet To Adopt a Sexual Assault Reporting App*, SLATE (Apr. 27, 2017, 5:04 PM), http://www.slate.com/blogs/xx_factor/2017/04/27/reporting_apps_like_callisto_are_offering_students_new_tools_for_dealing.html [<https://perma.cc/E64Y-JGQ7>].

61. See *I've-Been-Violated™*, WE-CONSENT, <http://we-consent.org/index.php/41-apps-abcd/103-i-ve-been-violated-app> [<https://perma.cc/C5D6-MR5C>].

62. *Id.*

63. *See id.*

64. See Claire Warner, *'Lighthouse' Independent Sexual Assault Reporting Website Might Change Everything, Although It Remains Controversial*, BUSTLE (June 9, 2016), <https://www.bustle.com/articles/165743-lighthouse-independent-sexual-assault-reporting-website-might-change-everything-although-it-remains-controversial> [<https://perma.cc/ZHK8-U453>].

65. *Id.*

66. *Id.*

gregated by the location of assaults,⁶⁷ as a medium-term goal.⁶⁸ This is consistent with global apps, such as Women Under Siege and HarassMap, which document instances of harassment on a map visualization.⁶⁹ Women Under Siege, which ceased updates in early 2016,⁷⁰ was a website that aggregated reports of rape in Syria. Anyone could file a submission, which required a written description of the incident including its location.⁷¹ Users were encouraged to use TOR and to provide supplemental evidence (that is, potential eyewitnesses, quotes, etc.).⁷² Egypt-based HarassMap, whose partners include Uber Egypt,⁷³ is a web-based platform where users can report incidents of both harassment and intervention.⁷⁴ When reporting harassment, the user must provide the location and specific description of the harassment. The platform is regularly reviewed “to make sure that the report is about sexual harassment” and about a *specific* incident.⁷⁵ Users are also encouraged to report instances of bystander intervention.⁷⁶ As it relates to prediction, trend analysis of aggregated data could inform prevention efforts — for instance, observing whether there are assault reports after a particular event.⁷⁷ However, it is important to note that these trends might not necessarily be causal: predictive power may be low, particularly if relatively low numbers of incidents are reported.

As one advocate points out, preventing assault is “only part of the point [These technologies] can help students get information

67. See Anya Kamenetz, *A Tech-Based Tool To Address Campus Sexual Assault*, NPR (Dec. 6, 2017, 6:00 AM), <https://www.npr.org/sections/ed/2017/12/06/567605752/a-tech-based-tool-to-address-campus-sexual-assault> (last visited May 5, 2018); Caplan-Bricker, *supra* note 60; Casey Fabris, *Callisto To Offer New Reporting System for Survivors of Sexual Assault*, CHRON. HIGHER EDUC. (Apr. 16, 2015), <https://www.chronicle.com/article/Callisto-to-Offer-New/229407> (last visited May 5, 2018).

68. See CALLISTO, *supra* note 52, at 9.

69. See Salamishah Tillet, *Apps (and Maps) To End Sexual Violence*, THE NATION (July 17, 2013), <https://www.thenation.com/article/apps-and-maps-end-sexual-violence/> [<https://perma.cc/4EKY-9GPR>]; see also SYLVIA WALBY ET AL., STOPPING RAPE: TOWARDS A COMPREHENSIVE POLICY 76 (2015) (citing Brazil, Haiti, and the U.N.’s use of mobile apps with geo-location technology for reporting and mapping).

70. See *Reports*, WOMEN UNDER SIEGE (Feb. 4, 2016, 9:09 PM), <https://womenundersiegesyria.crowdmap.com/reports/view/273> [<https://perma.cc/5XGS-Q42J?type=image>].

71. See *Submit a New Report*, WOMEN UNDER SIEGE, <https://womenundersiegesyria.crowdmap.com/reports/submit> [<https://perma.cc/9YQBS2HY?type=image>].

72. See *Digital Security & Submissions*, WOMEN UNDER SIEGE, <https://womenundersiege.syria.crowdmap.com/page/index/2> [<https://perma.cc/8NF5C6KD?type=image>].

73. See Tino Waked, *Uber Egypt’s Commitment To Prevent Sexual Harassment*, HARASSMAP (Nov. 9, 2017), <https://harassmap.org/en/news/uber-egypts-commitment-to-prevent-sexual-harassment> [<https://perma.cc/8CG6-NDCE>].

74. See *Share Your Story*, HARASSMAP, <https://harassmap.org/en/share-your-story> [<https://perma.cc/M2GG-N9GD>].

75. *Id.*

76. See *What Is Intervention*, HARASSMAP, <https://harassmap.org/en/what-intervention> [<https://perma.cc/9FH7-VENF>].

77. See Singer, *supra* note 59.

about resources when an assault does happen.⁷⁸ Nonprofit apps often provide a list of resources, alongside their reporting mechanisms.⁷⁹ These apps appear to be an improvement over web-based resources that schools provide. For instance, school websites may provide an overwhelming list of resources instead of clear, direct next steps,⁸⁰ which can be confusing and overwhelming.⁸¹ In contrast, the AskDC app, for example, shows steps that survivors can take as one-click buttons: talk to a counselor, obtain a survivor advocate, or schedule a visit for medical aid.⁸² AskDC's approach of providing clear next steps reduces the logistical costs for a survivor to find help and in turn, could encourage more students to come forward.

III. EVALUATION OF EXISTING APPLICATIONS

Successful technologies relating to sexual assault need to consider their downstream effects: Will potential targets use them? Will potential assailants be deterred by this increased usage? As stated in the Introduction, the concerns around the Shitty Media Men list focused on what features of technology best maximize reporting of accurate allegations and minimize reporting of false allegations. If an accuser's identity is anonymous, it could increase allegations overall, both true and false; conversely, if an accuser's identity is public, allegations might decrease overall.⁸³ Accordingly, technologies that seek to report sexual assault will need to consider this balance carefully and consider the legal issues around privacy.

If an app is insensitive to a survivor's experience or is clunky, it is unlikely that someone will wish to use it. Thus, technologies that prevent an assault from happening or encourage reporting will need to consider whether the apps actually do engage in prevention on the ground, and whether potential targets or survivors are willing to use the app. If there is little to no usage, the effectiveness of apps will also be quite low.

78. Summers, *supra* note 29.

79. See Kassien, *supra* note 30.

80. See, e.g., *Get Help for Sexual Violence*, U. MINN. ROCHESTER, <https://r.umn.edu/get-help-sexual-violence> [https://perma.cc/Y248-977K].

81. See Carol Smith, *Overwhelmed and Unsure, Victims Often Delay Seeking Help*, INVESTIGATEWEST (Feb. 25, 2010), <http://www.invw.org/2010/02/25/overwhelmed-and-unsure-vi/> [http://perma.cc/9W7F-F4AU]; see also generally CASS SUNSTEIN & RICHARD THALER, *NUDGE*, 9–10 (2008) (explaining how an overwhelming number of options can lead an individual to make bad choices).

82. See Sarah Rich, *App Helps Victims Report Sexual Assault Anonymously in D.C.*, GOV'T TECH. (Aug. 19, 2013), <http://www.govtech.com/health/App-Helps-Victims-Report-Sexual-Assault-Anonymously-in-DC.html> [https://perma.cc/C6BA-H8UB]; Brensilber, *supra* note 51.

83. This was the intuition for making the list anonymous. See Donegan, *supra* note 12.

A. Privacy

This Section evaluates the existing technologies using the Fair Information Practice Principles (“FIPPs”), commonly cited guideline for fair information practice,⁸⁴ to frame the discussion around privacy and security. The FIPPs consist of four values — Notice, Choice, Action, and Security⁸⁵ — as developed by governments in the United States, Canada, and Europe in the 1970s.⁸⁶ While the United States does not have a codified, uniform set of privacy principles,⁸⁷ the four FIPPs are the basis for the privacy policies of several federal agencies through the implementation of the Privacy Act of 1974.⁸⁸ Additionally, sector-specific statutes based on the FIPPs have been enacted in the United States.⁸⁹ The fact that the agencies’ application of the FIPPs closely tracks and overlaps with other fair information practice standards in other jurisdictions, such as the OECD’s Privacy Principles,⁹⁰ further supports the use of the FIPPs as the standard for this Note’s privacy analysis.

1. Notice and Choice

Under the Notice principle, consumers should receive “clear and conspicuous notice of [websites’] information practices, including

84. See Kenneth Bamberger & Deirdre Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 254 (2011).

85. See FED. TRADE COMM’N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE iii (2000).

86. See FED. TRADE COMM’N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998).

87. See *An Unprincipled Future? The Conflict Between FIPPs and the Internet of Things*, BERKELEY TECH. L.J. (June 22, 2016), <http://btlj.org/2016/06/an-unprincipled-future-the-conflict-between-fipps-and-the-internet-of-things/> [<https://perma.cc/8AZ8-J9X2>]; see also Bamberger & Mulligan, *supra* note 84, at 254 (“Legal academics and privacy experts have labeled the U.S. approach ‘FIP[Ps]-Lite.’”).

88. See, e.g., *IRS Privacy Policy*, INTERNAL REVENUE SERV., <https://www.irs.gov/privacy-disclosure/irs-privacy-policy> [<https://perma.cc/ZWF9-8QUM>] (last updated Sept. 18, 2017); *Our Privacy Principles*, CENSUS BUREAU, https://www.census.gov/about/policies/privacy/data_protection/our_privacy_principles.html [<https://perma.cc/Q2TU-X53Q>] (last updated Oct. 10, 2014).

89. See, e.g., parts of the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Financial Services Modernization Act. See Fred H. Cate, *The Failure of Fair Information Practice Principles*, in CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY, 358–59 (Jane K. Winn, Ed. 2006). Note that without a statute, the application of FIPPs in other settings typically relies on industry self-regulation. See generally Ira Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J.L. & POL’Y 356 (2011).

90. ORGANISATION FOR ECON. CO-OPERATION & DEV., THE OECD PRIVACY FRAMEWORK (2013), [hereinafter OECD] https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [<https://perma.cc/7CEA-3KVN>]; see also Memorandum from Hugo Teufel III, Chief Privacy Officer, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (Dec. 29, 2008) [hereinafter Privacy Policy Guidance Memorandum].

what information they collect, how they collect it, . . . how they use it, . . . whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.”⁹¹ Under the Choice principle, “sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided,”⁹² whether it be used inside or outside of the sites.

The Notice-and-Choice regime forms the regulatory model for privacy in the United States.⁹³ That is, an app or platform that collects information — whether it is collecting recordings of consent or reports of assault — would need to make sure its users understand who has access to the data and how it will be used. However, the empirical literature suggests that consumers may not understand the notice they are given and may inadvertently share their information as a result.⁹⁴ Second, the convenience and facade of anonymity that electronic reporting provides could make a user more likely to overlook dense legal writing. If reporting an assault electronically feels less triggering to a survivor,⁹⁵ she may over-trust the platform and share more information⁹⁶ without carefully reading how that information will be used.

Similarly, users of reporting apps might wrongly believe that something will be immediately done by the app, rather than the institution that the app reports to (either emergency services in a preven-

91. FED. TRADE COMM’N, *supra* note 85, at iii. This is similar to the OECD’s Purpose Specification Principle, which states that “[t]he purposes for [collection] should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.” OECD, *supra* note 90, at 14. Presumably, Notice may incorporate some aspects of the OECD’s Openness Principle, in which “[m]eans should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.” *Id.* at 15. The Notice principle also seems consistent with the OECD’s Accountability Principle, which states that “a data controller should be accountable for complying with measures which give effect to the [other privacy] principles.” *Id.* The Department of Homeland Security labels notice as a Transparency principle. See DEP’T OF HOMELAND SECURITY, *supra* note 90, at 3.

92. FED. TRADE COMM’N, *supra* note 80, at iii. The Choice principle roughly maps onto the OECD’s Collection Limitation and Use Limitation Principles, which advise that “data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.” OECD, *supra* note 85, at 14; see also Privacy Policy Guidance Memorandum, *supra* note 85.

93. Florencia Marotta-Wurgler, *Understanding Privacy Policies: Content, Self-Regulation, and Markets* 1–2 (N.Y.U. L. Sch. Law & Economics Research Paper Series Working Paper No. 16-18, 2016).

94. See OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW 6–8 (2014).

95. In creating an app, University of Pennsylvania administrators pointed out that students may be more comfortable with disclosure via texts rather than in person. See Brensilber, *supra* note 51.

96. As one nonprofit leader observes, “there’s no such thing as absolute confidentiality.” Fabris, *supra* note 67.

tion setting, or a university or HR department in a reporting setting). That is, there may be confusion about who the relevant authority is.⁹⁷ This distinction may be particularly important as between criminal cases and university adjudications; as one police officer noted, specific information that can prove guilt beyond a reasonable doubt in a charging decision might be better extracted from a trauma-informed officer or interviewer compared to an app, whereas the information collected by Callisto might suffice for the “preponderance of the evidence” standard in the Title IX context.⁹⁸ Confusion regarding the relevant authority may be problematic, if, for instance, an individual wishes to report to the police in the future, but only answers the prompts at the bare minimum to avoid further traumatization — she may think her incomplete account is sufficient.⁹⁹ Additionally, other offenses that might surface from a matching function might not be admissible in court.¹⁰⁰

Moreover, it may not be clear who has control of the data. In the context of Notice and Choice, individuals have to decide whether to trust certain technologies, and what sources of information they should use to evaluate these technologies before they consent to sharing their information. The National Network to End Domestic Violence (“NNEDV”) advises survivors to look at the source of the app: “If developed by a company that does not have expertise [around assault or abuse], it is likely that the app may contain information and suggestions that are not actually considered safe or recommended by experts.”¹⁰¹ With regard to privacy settings, NNEDV asks app developers: “Does the app work the way it is intended? . . . Are disclaimers included to inform survivors of possible safety risks? . . . Does the app description imply that it does more than the app actually provides?”¹⁰² For instance, one of the main concerns with the I’ve-Been-Violated

97. See, e.g., Tobias Salinger & Laura Bult, *What You Should Know About Reporting Sexual Assault on Campus*, N.Y. DAILY NEWS (Aug. 22, 2016), <http://www.nydailynews.com/news/national/reporting-sex-assault-campus-article-1.2759279> (last visited May 5, 2018).

98. See Madelyn Reese, *New Applications Aim To Transform and Aid Reporting of Sexual Assault*, DAILY U. WASH. (May 6, 2016), http://www.dailyuw.com/news/article_7f23fc86-1339-11e6-90b7-07b5ba475d9e.html (last visited May 5, 2018).

99. Cf. Sara F. Dudley, *Paved with Good Intentions: Title IX Campus Sexual Assault Proceedings and the Creation of Admissible Victim Statements*, 46 GOLDEN GATE U. L. REV. 117, 135 (2016) (“Unfortunately for a campus survivor, life has created circumstances where it may be easier to intentionally omit or falsify a shameful detail than be entirely candid with authorities. This erodes a survivor’s credibility with authorities and contributes to the creation of incomplete or inaccurate victim statements.”).

100. See Fabris, *supra* note 67.

101. Nat’l Network To End Domestic Violence, *Safety in a Mobile World: A Look at Apps*, TECH. SAFETY, <https://www.techsafety.org/lookatapps/> [<https://perma.cc/9TSN-AUGL>].

102. Nat’l Network To End Domestic Violence, *Considerations for App Developers: Safety & Privacy for Survivors of Abuse*, TECH. SAFETY, <https://www.techsafety.org/appdevelopers/> [<https://perma.cc/5WBW-QEBX>].

app was that it was not necessarily clear who benefited from the app; its creator, the Institute for the Study of Coherence and Emergence had no clear expertise assault issues.¹⁰³ Further, the fact that the app was previously packaged with other apps that included We-Consent and charged fees could seem exploitative.¹⁰⁴

Similarly, Lighthouse appears to have no formal institutional partners yet lists schools that a user can report to. While formal institutional partners might not be required per se, several colleges sent cease-and-desist letters so that Lighthouse would remove their names from its website.¹⁰⁵ Lighthouse's claim that its reporting data "is encrypted and separate, so the company 'couldn't pull [a] report together if [it] wanted to'" also seems at odds with the statement that it in fact pulls together reports for officials to view.¹⁰⁶ In contrast, in the workplace harassment app StopIt, "[s]ince multiple HR employees receive the reports, their handling is less subjective, and there's a smaller chance that a report might dead-end with a single HR worker,"¹⁰⁷ in theory leading to faster investigation turnarounds.

103. See *About Us*, INST. FOR STUDY COHERENCE & EMERGENCE, <http://www.isce.edu/index-5.html> [<https://perma.cc/5KLLK-AGPD>].

104. The reported fees for I've-Been-Violated and We-Consent have varied. At the time of its launch, We-Consent appeared to cost \$5 for a yearly membership. See Meg Graham, *New Apps Urge Mutual Consent, 'Yes Means Yes,' When It Comes to Sex*, CHICAGO TRIBUNE (July 25, 2015, 5:30 AM), <http://www.chicagotribune.com/bluesky/originals/ct-we-consent-app-michael-lissack-bsi-20150720-story.html> [<https://perma.cc/QB4E-ZG94>]. Later, We-Consent and I've-Been-Violated became free apps, while other apps called Party-Pass (an electronic consent pledge) and What-About-No charged \$5 per download. See Ciara O'Callaghan, *Mobile App "I've-Been-Violated" Helps Those Affected by Sexual Assault*, PENN STATE DAILY COLLEGIAN (Mar. 18, 2016), http://www.collegian.psu.edu/news/campus/article_a2257d7a-ec76-11e5-ba61-93bdc6eca2b4.html [<https://perma.cc/TZJ7-RUXZ>]; see also *Party Pass*, WE-CONSENT, <http://we-consent.org/index.php/41-apps-abc/104-party-pass-appwha> [<https://perma.cc/Q5JB-VCCX>] (description of Party-Pass); *What About No*, WE-CONSENT, <http://we-consent.org/index.php/41-apps-abc/102-what-about-no-app> [<https://perma.cc/9EM8-QG4V>] (descriptions of What-About-No). At various points, the suite of four apps appeared to be priced as a \$5 bundle. See Aleah Milliner, *Sexual Abuse Victims Will Have a Way To Record Evidence Through Free iTunes App*, THE U. DAILY KANSAN (Feb. 2, 2016), http://www.kansan.com/news/sexual-abuse-victims-will-have-a-way-to-record-evidence/article_4795d71c-c9ec-11e5-9c7a-07fea36fc415.html [<https://perma.cc/9GN2-T9Q3>]; Katherine Speller, *Do Consent Apps Really Work? Here's Why It Doesn't Matter*, MTV (July 29, 2015), <http://www.mtv.com/news/2226330/consent-theres-an-app-for-that/> [<https://perma.cc/M42L-4G3B>]. Currently, there is no fee to download I've-Been-Violated or We-Consent. See *Apps Are Free*, WE-CONSENT, <http://we-consent.org/index.php/get-the-app-suite> [<https://perma.cc/F3SR-L6XR>].

105. See Tyler Kingkade, *Why Colleges Are Worried About a New Sexual Reporting Website*, HUFFINGTON POST (Feb. 2, 2017), https://www.huffingtonpost.com/entry/rape-reporting-website-colleges_us_5720e4b5e4b0b49df6a9c8c4 (last visited May 5, 2018).

106. Warner, *supra* note 59.

107. Greenfield, *supra* note 32.

2. Access

Under the Access principle, consumers should have “reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.”¹⁰⁸ Here, the most intuitive interpretation of when the Access principle might be violated is in the case of false accusations. This could theoretically occur for two reasons. First, consider the probability in the Callisto app that two individuals incorrectly name the same assailant, “John Smith,” resulting in a report being erroneously sent to a university. Currently, Callisto attempts to correct for this error by requesting a unique ID (a Facebook URL to avoid matching common names),¹⁰⁹ but the assailant may look similar to or may have pretended to be John Smith. However, if the real John Smith is able to show that he was perhaps somewhere else at the time, in a criminal adjudication, this issue could be clarified at the point of investigation even without changes to the platform.

More ominously, one might consider a deliberate effort to accuse an individual. Based on the fact that technology appears to reduce the cost of reporting, we could expect that false accusations might increase.¹¹⁰ However, this does not account for (1) the low rate of false accusations overall,¹¹¹ which might be in turn due to the fact that accusers, in addition to making a report, may have to engage in other time-consuming efforts related to their accusation,¹¹² (2) undercount-

108. FED. TRADE COMM’N, *supra* note 85, at iii; *see also* OECD, *supra* note 90, at 14 (“Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.”); Privacy Policy Guidance Memorandum, *supra* note 85, at 4 (“DHS should, to the extent practicable, ensure that PII [personally identifiable information] is accurate, relevant, timely, and complete.”). The Access principle also parallels the OECD’s Individual Participation Principle. *See* Privacy Policy Guidance Memorandum, *supra* note 85, at 3 (“DHS should involve the individual in the process of using PII [personally identifiable information] and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS’s use of PII.”)

109. *See Reporting Options*, CALLISTO, <https://stanford.callistocampus.org/reporting/> [<https://perma.cc/RB78-VG69>].

110. *Cf.* Lee & Suen, *supra* note 83, at 3 (suggesting a real victim is more inclined to delay the cost of reporting while a libeler may come forward immediately).

111. *See* David Lisak et al., *False Allegations of Sexual Assault: An Analysis of Ten Years of Reported Cases*, 16 VIOLENCE AGAINST WOMEN 1318, 1318 (2010).

112. *See* Michaela Cross, *How Campus Rape Victims Get Hurt by the Laws That Are Supposed To Protect Them*, VICE (June 6, 2016, 1:22 AM), https://www.vice.com/en_us/article/nkj48/how-campus-rape-victims-get-hurt-by-the-laws-that-supposed-to-protect-them-title-ix [<https://perma.cc/F9VH-4S2C>].

ing,¹¹³ and (3) the fact that false reports are likely to be made at a lower rate than accurate reports.¹¹⁴

In certain databases, such as the Shitty Media Men spreadsheet, it may seem problematic that anonymous individuals might contribute to a database of misconduct. However, the specificity of the claim should allow individuals to make their own judgments about whether that claim is true or not. For instance, with HarassMap, moderators regularly check the site to make sure that reports of harassment are specific to a location or behavior, in order to limit the possibility of false accusations.¹¹⁵

Another take on Access might question whether an individual should even know that there is data that relates to an accusation against them. A reporting system, including perhaps a “whisper network,” assumes that if a harasser knew they were being gossiped about, they might curb or become more subtle in their behavior (i.e. a deterrent effect).¹¹⁶ One could imagine that a serial harasser would be deterred from continuing his or her behavior if this information became public.

3. Security

Finally, “sites would be required to take reasonable steps to protect the security of the information they collect from consumers.”¹¹⁷ Under the OECD Framework, reasonable steps are aimed against “loss or unauthorised access, destruction, use, modification or disclosure of data.”¹¹⁸ While all of the reporting platforms state that their data is encrypted,¹¹⁹ an encrypted database is not impossible to access, particularly if an individual is motivated enough.¹²⁰ Also, while no

113. See Corey Yung, *How To Lie with Rape Statistics: America's Hidden Rape Crisis*, 99 IOWA L. REV. 1197, 1204 (2014).

114. See Lee & Suen, *supra* note 83, at 3.

115. See *Share Your Story*, *supra* note 74.

116. See Conor Friedersdorf, *How To Identify Serial Harassers in the Workplace*, THE ATLANTIC (Nov. 28, 2017), <https://www.theatlantic.com/politics/archive/2017/11/whisper-networks-20/546311/> [<https://perma.cc/8GXH-UVE2>].

117. FED. TRADE COMM'N, *supra* note 86, at iii.

118. OECD, *supra* note 90; cf. DEP'T OF HOMELAND SECURITY, *supra* note 90 (“DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.”).

119. See, e.g., *What We Do*, CALLISTO, <https://www.projectcallisto.org/what-we-do> [<https://perma.cc/P65B-WUUY>]; *Core Features*, LIGHTHOUSE, <http://lighthouse.vertigolabs.com/features.html> [<https://perma.cc/ZPS3-XFUN>]; Google Play, *I've-Been-Violated*, <https://play.google.com/store/apps/details?id=edu.isce.violated&hl=en> [<https://perma.cc/P65B-WUUY>].

120. See Anna North, *A New Way To Report College Sexual Assault*, N.Y. TIMES: TAKING NOTE (May 27, 2016, 2:50 PM), <https://takingnote.blogs.nytimes.com/2016/05/27/a-new-way-to-report-college-sexual-assault> [<https://perma.cc/TF7Z-D93T>].

anonymous information is necessarily revealed, aggregated data might reveal specific information inadvertently. Consider, for example, a map that indicates a relatively small number of incidents in a specific location. A defendant who has participated in an incident in that location may be more likely to believe someone has accused them — should he or she somehow obtain access to this information.¹²¹ Alternatively, given that demographic data is collected in Callisto and Lighthouse,¹²² knowing the race of a survivor might narrow down whether he or she has reported. Now consider the theoretical example of a university that is not particularly racially diverse. If a survivor of color reports her assault to an app or platform that collects demographic data, it may be possible to identify who made the report. In particular, when other data is present (e.g., location), the ability to de-anonymize a report becomes significantly increased.

4. Incentives to Adopt Technological Interventions

Altogether, this FIPPs framework allows us to briefly consider the privacy mechanics of these technologies. However, one outstanding question concerns accountability: who is liable for the downstream consequences? One intuition is that employers or universities would not want to adopt any of these technologies. As the founder of Callisto asserted, some tech companies declined to use the app not only because “[t]hey’re nervous about having a third party collect data,” but also because “[t]hey don’t want to know.”¹²³ First, if an employer hosts a database of accusations, they might be liable for libel under certain conditions.¹²⁴ This concern might be alleviated by the presence of a third-party escrow to which the liability would pass.

Second, employers are obligated to investigate claims of harassment by supervisors, depending on the circumstances.¹²⁵ Similarly, case law indicates if universities know of problematic areas on campus, a lack of corrective action might be viewed as a lack of “reasonable care.”¹²⁶ But without that information, they may not have to

121. Even if that is somewhat illogical statistically, assuming that the defendant does not have baseline data.

122. See *Our Policies*, CALLISTO, <https://stanford.callistocampus.org/about/our-policies/> [<https://perma.cc/56FH-7CE9>]; Warner, *supra* note 64.

123. See Sara Ashley O’Brien, *She Wants Her Rape Reporting Software To Be Universal*, CNN (Mar. 31, 2017, 12:44 PM), <http://money.cnn.com/2017/03/31/technology/callisto-sexual-assault-software/index.html> [<https://perma.cc/NW2G-KXXS>].

124. See Huet & Bergen, *supra* note 49.

125. See U.S. EQUAL EMP. OPPORTUNITY COMM’N, ENFORCEMENT GUIDANCE ON VICARIOUS EMPLOYER LIABILITY FOR UNLAWFUL HARASSMENT BY SUPERVISORS (1999), available at <https://www.eeoc.gov/policy/docs/harassment.html> [<https://perma.cc/8V9N-C62L>].

126. See *id.* (collecting cases); see also *Mullins v. Pine Manor C.*, 449 N.E.2d 331, 336 (Mass. 1983) (“Parents, students, and the general community still have a reasonable expect-

dedicate resources to address the issue, both in terms of money and time.¹²⁷ Still, however, the threat of high-profile cases may change institutions' outlook: public press tied Stanford's adoption of Callisto with the Brock Turner case.¹²⁸ And there is a possibility that universities have an obligation to gather information about their employees and students.¹²⁹ Another suggestion might be for law enforcement to partner with or adopt these technologies,¹³⁰ given that it could lead to more effective use of resources.

B. Increasing Take-Up

If after a university adopts one of these technologies it desires more preventative or predictive power around assault, then it will need to increase take-up of the app, that is, encourage survivors to report otherwise unreported experiences. Moreover, high take-up may also create a social norm in which it may not be clear whether someone with the app is a bystander or survivor, which could enhance reporting rates.¹³¹

Additionally, increasing take-up might be important because if only a few individuals use the app, then the use of the tool will heavily rely on the veracity of these few reports.¹³² As a result, the tool might privilege certain types of survivors or narratives in the same way that prevention tools might reinforce stereotypes. In particular, several professors have expressed concerns about Harvard University's misconduct policy because it could have a "disproportionate impact on racial minorities of discipline for campus sexual misconduct."¹³³ That disproportionate impact may come from a

tation, fostered in part by colleges themselves, that reasonable care will be exercised to protect resident students from foreseeable harm."); *see generally* Andrea Curcio, *Institutional Failure, Campus Sexual Assault and Danger in the Dorms*, 78 MONT. L. REV. 31 (2017) (analyzing campus sexual assault and schools' duty to use precautionary measures to protect students living in dorms); *cf.* *Doe v. Emerson C.*, 153 F. Supp. 3d 506, 515 (D. Mass. 2015) ("[I]t does not follow that Emerson could reasonably be expected to anticipate and prevent a sexual assault occurring at an *off-campus* party.") (emphasis added).

127. *See generally* DEP'T. OF EDUC., Q&A ON CAMPUS SEXUAL MISCONDUCT (2017).

128. *See, e.g.*, Khari Johnson, *Stanford University To Pilot Sexual Assault Reporting Software Callisto*, VENTUREBEAT (Apr. 27, 2017, 10:56 AM), <https://venturebeat.com/2017/04/27/stanford-university-to-pilot-sexual-assault-reporting-software-callisto/> [<https://perma.cc/8F9S-ACY6>].

129. *See* Eugene Volokh, *Tort Law vs. Privacy*, 114 COLUM. L. REV. 879, 899–900 (2014).

130. *See* Fabris, *supra* note 67.

131. *See* Rich, *supra* note 82.

132. *See generally* Sarah Jane Brubaker et al., *Measuring and Reporting Campus Sexual Assault: Privilege and Exclusion in What We Know and What We Do*, 11 SOC. COMPASS e12543 (2017) (analyzing bias in sexual assault incident reporting).

133. Elizabeth Barholet et al., *Fairness for All Students Under Title IX*, DIGITAL ACCESS TO SCHOLARSHIP HARV. (Aug. 21, 2017), <https://dash.harvard.edu/bitstream/handle/>

skewed sample of reports. To address this concern, increasing take-up of technologies seems important to mitigate bias.

In particular, interventions should be inclusive of those individuals who may not have an obvious institution to which to express grievances. First, industry-wide spreadsheets might name employed individuals, but accusers might not work in the same company as the defendant, making reporting procedurally difficult. Similarly, gig economy and freelance workers, particularly when unionized, may not have protections given their contractor status.¹³⁴ Future interventions can and should be tailored to these networks.

As the *Washington Post* points out in its discussion of the Shitty Media Men spreadsheet,

[B]athroom and barroom warnings [have] passed between women for generations in written form. Those have long been the best hope of women seeking to shield themselves and their peers from sexual assault, because many feel that making a public accusation and allowing a man to respond rarely works, that using official channels rarely works, that even filing suit often doesn't work.¹³⁵

In this way, reporting technology is a modern form with several theoretical benefits: it reduces the social costs around reporting by allowing for the “matching” function of reports against the same person and for the ability to send an account electronically rather than recounting it in person.¹³⁶ It also reduces the logistical costs by allowing third-party verification for the timing of a survivor’s recollection and allowing for distribution quickly.

1/33789434/Fairness%20for%20All%20Students.pdf?sequence=1 [https://perma.cc/XEG4-VCFC].

134. See, e.g., *Jones v. A.W. Holdings, LLC*, 484 Fed. App'x 44, 48 (7th Cir. 2012); *Hunt v. State of Missouri, Dep't of Corr.*, 297 F.3d 735, 741 (8th Cir. 2002) (“The law is well established that Title VII protects employees, not independent contractors, from discriminatory employment practices.”). But see *Hunt*, 297 F.3d at 741 (“[T]he existence of a contract referring to a party as an independent contractor does not end the inquiry, because an employer may not avoid Title VII by affixing a label to a person that does not capture the substance of the employment relationship.”) (internal quotation marks omitted) (quoting *Schwieger v. Farm Bureau Ins. Co. of Neb.*, 207 F.3d 480, 483 (8th Cir. 2000)); see generally *Have You Experienced Harassment as a US Tech Employee or Worker in the Gig Economy?*, THE GUARDIAN (Aug. 23, 2017, 6:00 AM), <https://www.theguardian.com/business/2017/aug/23/share-your-experience-harassment-gig-economy-tech> [https://perma.cc/W2A8-QED5] (attempting to collect reports).

135. Molly Roberts, *How BuzzFeed Helped Turn a Secret List of Potential Abusers in Media into a Burn Book*, WASH. POST: POST PARTISAN (Oct. 12, 2017), <https://www.washingtonpost.com/blogs/post-partisan/wp/2017/10/12/how-buzzfeed-turned-a-secret-list-of-potential-abusers-in-media-into-a-burn-book/> (last visited May 5, 2018).

136. See generally Heidi Liu, *Do Androids Dream of Bad News?*, 15 CANADIAN J. L. & TECH. 109 (2017).

1. Design

Simple design principles are important in pursuit of the goal of increasing take-up.¹³⁷ As mentioned previously,¹³⁸ a list of resources can be overwhelming: while that might seem a small cost, the psychological literature suggests that it is these logistical tensions that might lead someone not to follow through on what they consider to be important actions.¹³⁹

As it relates to preventative technologies, consent app Good2Go is one example of poor design. As *Slate* described, not only do potential partners click through a series of screens for consent, but if one partner does not have the app downloaded, he or she must use her phone to verify her number — altogether taking four minutes.¹⁴⁰ Moreover, only one party's level of intoxication is recorded,¹⁴¹ which could be problematic as a potential assailant could simply claim he was drunk. Alternatively, he could persuade his potential partner to click "Intoxicated but Good2Go" instead of "Pretty Wasted," which would allow the app to proceed.¹⁴²

There are also differing opinions on the use of smartphones themselves in increasing take-up. The founder of Circle of 6 defends her smartphone app by stating that "[m]ost young people first report sexual assault to a friend or a peer, not to the police or a blue safety light . . . [a]nd they're always on their phone."¹⁴³ In contrast, Callisto removed its app feature because it felt survivors would be uncomfortable with having a visible app on their phones.¹⁴⁴ One academic paper that evaluated the information escrow mechanism underlying Callisto yielded survey evidence that individuals would be more likely not only to report an assault with the matching mechanism, but also possibly to make a formal complaint on their own.¹⁴⁵ That is, the option to report to Callisto does not cause survivors who might otherwise make a (informal or formal) complaint to simply store their report in

137. See Anwar, *supra* note 36.

138. See *supra* notes 80–81 and accompanying text.

139. For instance, individuals may hesitate in applying to college, see generally Adam Lavecchia, Heidi Liu & Philip Oreopoulos, *Behavioral Economics of Education*, in HANDBOOK OF THE ECONOMICS OF EDUCATION 1 (Eric A. Hanushek, Stephen Machin & Ludger Woessmann eds., 2016), or obtaining a flu shot, see generally Katy Milkman et al., *Using Implementation Intentions Prompts To Enhance Influenza Vaccination Rates*, 108 PNAS 10415 (2011).

140. See Hess, *supra* note 41.

141. See *id.*

142. Cf. *id.*

143. Summers, *supra* note 29.

144. See Cassie Werber, *The Culture of Secrecy That Fuels Campus Rape Has a Tech Solution*, QUARTZ (May 4, 2017), <https://qz.com/973539/the-culture-of-secrecy-that-fuels-campus-rape-has-a-tech-solution-called-callisto/> [<https://perma.cc/5NCS-VYLZ>].

145. See Ian Ayres, *Voluntary Taxation and Beyond: The Promise of Social-Contracting Voting Mechanisms*, 19 AM. L. & ECON. REV. 1, 39 (2017).

the system instead.¹⁴⁶ Comparing the relative reporting rates between a phone and web interface could be worthwhile.

2. Cultural Stereotypes of Harassment/Assault

A first-order objection to tools that primarily emphasize harassment/assault prevention is that it puts the onus on victims to ensure their own safety.¹⁴⁷ A related concern is that they may undermine privacy generally — simply allowing someone (even a friend) to follow one's walking path via iPhone requires a certain sacrifice of privacy. Even if the individual opts into this sort of technology, it can create an expectation that avoiding misconduct requires sacrificing privacy.

Moreover, preventative tools imply a particular stereotype of assault.¹⁴⁸ Many of those listed earlier¹⁴⁹ involve loud sounds and alerts, suggesting that the stereotypical assault comes from a stranger¹⁵⁰ — however, the majority of assaults are committed by someone the victim knows.¹⁵¹ Additionally, one of the primary objections to the I've-Been-Violated app, which records consent, is that consent can change at any time — accordingly, recording consent at any one point might be unrealistic or misleading and reinforce the stereotype that consent for one action implies consent for other actions.¹⁵² Indeed, the founder of I've-Been-Violated justified his use of the app name based on the claim that students otherwise “send each other vague signals on the assumption that the other person knows what you're talking about”¹⁵³ — reinforcing stereotypes about how targets might send “mixed signals.” The fact that We-Consent — launched by the same institution as I've-Been-Violated — “self-destructs” if someone says

146. *Id.*

147. See Sirin Kale, *The Complicated Promise of Anti-Rape Technologies*, VICE (Oct. 2, 2017, 10:26 AM), https://broadly.vice.com/en_us/article/xwg75j/the-complicated-promise-of-anti-rape-technologies (last visited May 5, 2018).

148. See generally Rena Bivens & Amy Adele Hasinoff, *Rape: Is There an App for That? An Empirical Analysis of the Features of Anti-Rape Apps?*, INFO., COMM. & SOC. (2017), <https://doi.org/10.1080/1369118X.2017.1309444> (last visited May 5, 2018) (conducting an empirical analysis of the features of anti-rape apps).

149. Summers, *supra* note 27.

150. See Tara Culp-Ressler, *Profit and Peril in the Anti-Rape Industry*, THINKPROGRESS (Sept. 10, 2014, 2:45 PM), <https://thinkprogress.org/profit-and-peril-in-the-anti-rape-industry-e497c017b0cc/> [<https://perma.cc/8E7N-28UW>].

151. See *Perpetrators of Sexual Violence: Statistics*, RAINN, <https://www.rainn.org/statistics/perpetrators-sexual-violence> [<https://perma.cc/K7BZ-H7BX>].

152. That is, one can imagine a bad actor asking for consent for one thing and using it to justify other acts. The easy remedy for this would be to record continuously, but that could require an unreasonable sacrifice of privacy, as described in the last paragraph. According to I've-Been-Violated and We-Consent's creator, the Apple App Store rejected the apps because they were “icky.” See Molly Petrilla, *Can An App Help Reduce Sexual Assault on College Campuses?*, FORTUNE (Sept 1, 2015), <http://fortune.com/2015/09/01/affirmative-consent-app/> (last visited May 5, 2018).

153. Reese, *supra* note 93.

no,¹⁵⁴ instead of providing a video record and sending an alarm — suggests that perhaps its use could be more beneficial for assailants.

The experience of survivors in using these tools should be of first-line importance. Emotional discomfort stemming from the app (as opposed to from the experience itself) is likely to decrease take-up of these tools. As one *Slate* contributing writer points out, “[t]he best sexual assault apps seem to be the ones that drastically speed things up and that monitor data in a way that analog reporting and counseling can’t. But technology alone can’t change the human dynamic at work here.”¹⁵⁵ In 2016, researchers from Stanford University and the University of California found that digital assistants (e.g., Apple’s Siri, Microsoft’s Cortana) did not recognize when an individual was looking for resources for sexual assault.¹⁵⁶ While this issue was immediately corrected — by directing most of the inquiries to the number of the National Sexual Assault Hotline¹⁵⁷ — critics suggested that these quick fixes were a symptom of a larger insensitivity.¹⁵⁸

3. Standards for Reporting

In contrast to the sensitivity problems described above, reporting apps like Callisto, HarassMap, or Women Under Siege allow someone to tell their specific story. For example, Callisto touts its trauma-centered approach.¹⁵⁹ Features of the platform include encouragement for the survivor to take breaks so as not to be overwhelmed, and for their description of the experience to not necessarily follow a linear pattern,¹⁶⁰ so that it may be easier to deal with recall. However, critics have pointed out that asking someone to look up their assailant on Facebook, as Callisto does, could be triggering,¹⁶¹ although Callisto stated that they had not seen that in their user survey feedback.¹⁶²

The ability to report narratives may cause the threat of backlash. Opponents of the anonymous reporting documents discussed above

154. See Apple, *supra* note 38.

155. Nora Caplan-Bricker, *This App for Victims of Sexual Assault Is a Terrible Idea — and It’s Not an Outlier*, SLATE (Jan. 19, 2016, 5:18 PM), http://www.slate.com/blogs/xx_factor/2016/01/19/app_for_victims_of_sexual_assault_is_a_terrible_idea_and_it_s_not_an_outlier.html (last visited May 5, 2018).

156. See Adam Miner et al., *Smartphone-Based Conversational Agents and Responses to Questions About Mental Health, Interpersonal Violence, and Physical Health*, 176 JAMA INTERNAL MED. 619, 623 (2016).

157. See Michael Nedelman, *Siri Now Understands Questions About Sexual Assault After Study Critiqued Automated Responses*, ABCNEWS (Mar. 30, 2016, 2:20 PM), <http://abcnews.go.com/Health/siri-now-understands-questions-sexual-assault-study-critiqued/story?id=38031759> [<https://perma.cc/PRQ2-JVS7>].

158. See, e.g., SARA WACHTER-BOETTCHER, TECHNICALY WRONG 6 (2017).

159. See Callisto, *supra* note 49, at 3.

160. See *id.*

161. See Singer, *supra* note 55.

162. *Id.*

might call this “political correctness” run amok, since the behaviors cited in the “Shitty Media Men” spreadsheet ranged from misogynistic behavior to felony assault,¹⁶³ and the “Yes, at Google” email list included things that might not rise to the level of unlawful harassment.¹⁶⁴ A relatively low-barrier solution to this objection would be for reporting apps to provide information on what *is* a criminal act in the state that the user is located. It seems extremely likely that many non-lawyers might not understand that criminal statutes are determined at the state level, and that there are different wordings for each sort of crime. Similarly, for actions that do not necessarily fall under a criminal statute, reporting apps can provide information on which behaviors are problematic even if they may not be punishable by a court or institution.

On the other hand, one potential issue with a codified system of reporting is that “[i]t might allow people who have survived sexual assault to get over the first-mover disadvantage, but it may also codify an entrenched attitude that women need to have corroborating evidence to be believed.”¹⁶⁵ Consider the earlier example in which an individual reports the bare minimum to avoid retraumatization.¹⁶⁶ If she later adds more information, it seems possible that the time-stamped entry will account for that revision, and could be misperceived as her revising her account. To that extent, cultural change might be necessary. The #MeToo movement may reflect that cultural change may be underway¹⁶⁷: even though many of the recent harassment claims required significant numbers of survivors to speak up, one might suggest that the multiplicity of claims lowers the social and logistical barriers for an individual claim to be raised. Finally, what should lawmakers do, given that repeat offenders likely and deliberately target women who they believe are less likely to report an assault?¹⁶⁸ Does this enhance the promise of predictive technologies?

IV. CONCLUSION

This Note examined the current scope of technologies around sexual assault. Altogether, the use of these technologies highlights the

163. See Shafir, *supra* note 1.

164. See Huet & Bergen, *supra* note 47.

165. Singer, *supra* note 55.

166. See *supra* Section III.A.1.

167. See, e.g., Jodi Kantor & Megan Twohey, *Harvey Weinstein Paid Off Sexual Harassment Accusers for Decades*, N.Y. TIMES (Oct. 5, 2017), <https://www.nytimes.com/2017/10/05/us/harvey-weinstein-harassment-allegations.html> (last visited May 5, 2018); Abby Ohlheiser, *How #MeToo Really Was Different, According to Data*, WASH. POST (Jan. 22, 2018, 4:22 PM), <https://www.washingtonpost.com/news/the-intersect/wp/2018/01/22/how-metoo-really-was-different-according-to-data> (last visited May 5, 2018).

168. See generally Amy Blackstone, Christopher Uggen & Heather McLaughlin, *Legal Consciousness and Responses to Sexual Harassment*, 43 L. & SOC. REV. 631 (2010).

tension in attempting to reconcile the needs of a survivor and the needs of the legal system. The rhetoric around these technologies relies heavily on a discussion of changing the existing culture from that of “rape culture.” The developers of these technologies do not necessarily guarantee that the action an institution takes will be satisfactory to the individual.¹⁶⁹ Instead, advocates argue that the tools “do something more.”¹⁷⁰ “They innovatively engage and redefine the bystander as friends, guardians, survivors of gender-based violence, volunteers and witnesses, in order to reduce the likelihood of individual and collective acts of sexual violence.”¹⁷¹

In the years since the 2011 Dear Colleague letter that laid out standards for university investigations of sexual assault,¹⁷² commentators have argued that harassment prevention is “now an exploding industry with everything from fingernail polish that detects date-rape drugs in drinks to necklaces that hide mini panic buttons — and all kinds of crash courses on how to get and give consent.”¹⁷³ Although the Department of Education withdrew guidance around sexual assault reporting in universities earlier this year Still, although the Department of Education withdrew guidance around sexual assault reporting in universities earlier this year,¹⁷⁴ it seems important to evaluate the claims of these technologies — whether well-intentioned or not — in an evidence-based fashion, given the “watershed moment” of recent disclosures of harassment.¹⁷⁵

There will — at least for a while — be new tools to evaluate. As Jia Tolentino states:

Speech about sexual assault can stem from a variety of worthy motivations: to warn other women, to find closure and catharsis, to enact or perform solidarity, to get an abusive person out of a position of power, to change institutional procedures. These goals can overlap, and they often do — but not automatically . . . It would help . . . if we understood that at-

169. “It’s not just about the specific bystander skills, it’s building a culture that is less accepting and less tolerant of sexual violence.” Summers, *supra* note 27.

170. Tillet, *supra* note 64.

171. *Id.*

172. See generally DEP’T. OF EDUC., DEAR COLLEAGUE LETTER (2011), *supra* note 22.

173. See Smith, *supra* note 27.

174. Department of Education Issues New Interim Guidance on Campus Sexual Misconduct, DEP’T OF EDUC. (Sept. 22, 2017), <https://www.ed.gov/news/press-releases/department-education-issues-new-interim-guidance-campus-sexual-misconduct> [<https://perma.cc/Y3W4-HZ29>].

175. Jessica Taylor, *Speaker Ryan on Sexual Harassment: “We Are Having a Watershed Moment in This Country”*, NPR (Nov. 30, 2017, 5:59 PM), <https://www.npr.org/2017/11/30/567588841/speaker-ryan-on-sexual-harassment-we-are-having-a-watershed-moment-in-this-count> (last visited May 5, 2018).

tempts to repair a flawed system are unlikely to be either perfect or categorically wrong.¹⁷⁶

176. Tolentino, *supra* note 2.