

INTIMATE SURVEILLANCE

KAREN E.C. LEVY*

TABLE OF CONTENTS

I. INTRODUCTION: NORMALIZING INTIMATE SURVEILLANCE	679
II. WHAT THIS ARTICLE IS NOT ABOUT	680
III. THE LIFE COURSE OF INTIMATE SURVEILLANCE.....	681
A. Dating: Scoping Out Potential Intimates.....	682
B. Tracking Intimate and Romantic Practices.....	683
C. Monitoring Fertility.....	684
D. Surveillance, Abuse, and Revenge.....	686
IV. RISKS AND IMPLICATIONS.....	687
A. Quantification as Objectivity, Measurement as Control	687
B. Monitoring, Trust, and Intimate Values	689
C. Privacy Risks.....	689
V. CONCLUSION	692

I. INTRODUCTION: NORMALIZING INTIMATE SURVEILLANCE

Data collection and analytics have pervaded nearly every sphere of daily life, from commerce¹ to health², from transport³ to education,⁴ to employment.⁵ Accompanying the data imperative is an emergent social paradigm: the normalization of surveillance across contexts and scales. Even what we think of as our most personal relationships are not immune to data's infiltration, as we come to define and manage these relations through data exchange,⁶ and to quantify and analyze the most mundane aspects of our daily existence in incredibly fine-grained detail;⁷ social

* Postdoctoral Fellow, Information Law Institute, New York University School of Law and Department of Media, Culture, and Communication, New York University. Fellow, Data & Society Research Institute. I gratefully acknowledge financial support from the Intel Science and Technology Center for Social Computing (ISTC-Social). Thanks to Amanda Levendowski, Alex Rosenblat, Sofia Jawed-Wessel, and Dave Johns for suggestions and advice.

1. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 19, 2012, at MM30, available at <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.

2. David W. Bates et al., *Big Data in Health Care: Using Analytics to Identify and Manage High-Risk and High-Cost Patients*, 33 HEALTH AFF. 1123, 1123–24 (2014).

3. Adele Peters, *Boston is Using Uber Data to Plan Better Urban Transportation*, CO.EXIST (Jan. 16, 2015, 1:10 PM), <http://www.fastcoexist.com/3040964/boston-is-using-uber-data-to-plan-better-urban-transportation>.

4. Lisa Fleisher, *Big Data Enters the Classroom*, WALL. ST. J. (Mar. 23, 2014, 4:35 PM), <http://www.wsj.com/articles/SB10001424052702304756104579451241225610478>.

5. Steve Lohr, *Unblinking Eyes Track Employees*, N.Y. TIMES (Jun. 21, 2014), <http://www.nytimes.com/2014/06/22/technology/workplace-surveillance-sees-good-and-bad.html>.

6. Karen E.C. Levy, *Relational Big Data*, 66 STANFORD L. REV. ONLINE 73 (2013), available at <http://www.stanfordlawreview.org/online/privacy-and-big-data/relational-big-data>.

7. Dawn Nafus & Jamie Sherman, *This One Does Not Go Up to 11: The Quantified Self Movement as an Alternative Big Data Practice*, 8 INT'L J. COMM. 1784 (2014); Anne Helen Petersen, *Big Mother is Watching You*, BUZZFEED (Jan. 1, 2015, 9:43 AM), <http://www.buzzfeed.com/annehelenpetersen/the-track-everything-revolution-is-here-to-improve-you-wheth>.

surveillance has become the rule.⁸ This article examines the rise of the surveillant paradigm within some of our most intimate relationships and behaviors—those relating to love, romance, and sexual activity—and considers what challenges this sort of data collection raises for privacy and the foundations of intimate life.

Data-gathering about intimate behavior was, not long ago, more commonly the purview of state public health authorities, which have routinely gathered personally identifiable information in the course of their efforts to (among other things) fight infectious disease.⁹ But new technical capabilities, social norms, and cultural frameworks are beginning to change the nature of intimate monitoring practices. Intimate surveillance is emerging and becoming normalized as primarily an *interpersonal* phenomenon, one in which all sorts of people engage, for all sorts of reasons. The goal is not top-down management of populations, but establishing knowledge about (and, ostensibly, concomitant control over) one's *own* intimate relations and activities.¹⁰

After briefly describing some scope conditions on this inquiry, I survey several types of monitoring technologies used across the “life course” of an intimate relationship—from dating to sex and romance, from fertility to fidelity, to abuse. I then examine the relationship between data collection, values, and privacy, and close with a few words about the uncertain role of law and policy in the sphere of intimate surveillance.

II. WHAT THIS ARTICLE IS NOT ABOUT

The nexus between sexuality and technology is an area of rapid growth and evolution, and one that presents a number of unique challenges to legal regulation. This Article does not attempt to elucidate the entire range of emergent sexual surveillance practices; in consideration of the focus of the Symposium, it focuses generally on practices occurring within the home, often (though not always) between consensual partners. Even with this scope in mind, the list of surveillance tools and practices I discuss in Section III is not intended to be exhaustive. Still, in light of the importance of some intimate surveillance issues this Article does *not* discuss, I explicitly note here some of the practices I bracket from my analysis. These issues are pressing and complex, and deserving of their own careful treatment by policy-makers, legal scholars, and social scientists.

For one, this article is not about the relationship between technology and sex work (i.e., the provision of sexual services for payment) or sex trafficking. A good deal of promising research is emerging on the role of technology in sex work and sex trafficking—including both the use of mobile phones and social media to facili-

8. See Alice E. Marwick, *The Public Domain: Surveillance in Everyday Life*, 9 SURVEILLANCE & SOC'Y 378, 385 (2012).

9. Amy Fairchild et al., *Public Goods, Private Data: HIV and the History, Ethics, and Uses of Identifiable Public Health Information*, 122 PUB. HEALTH REP. 7 (2007); AMY L. FAIRCHILD ET AL., SEARCHING EYES: PRIVACY, THE STATE, AND DISEASE SURVEILLANCE IN AMERICA (2007).

10. Levy, *supra* note 6; see also Woodrow Hartzog & Evan Selinger, *Big Data in Small Hands*, 66 STAN. L. REV. ONLINE 81, 83 (2013) (“Individuals eventually will be able to harness big datasets, tools, and techniques to expand dramatically the number and magnitude of privacy harms to themselves and others This is problematic in an age when so many aspects of our social relationships with others are turned into data.”).

tate trafficking¹¹ and the use of new analytic techniques to combat the sex trade.¹² *The Economist* recently analyzed nearly 200,000 social media profiles of female sex workers online to produce a “big data” analysis of the economics of commercial sex.¹³ Because sex trafficking and sex work take place largely outside the domestic sphere and pose unique technical, social, and legal problems, I exclude them from my discussion here.

Second, this article does not attempt to analyze the dynamics of online sex scandals or the problem of online sexual harassment, such as the massive celebrity nude photo hack of 2014 (known popularly as “The Fappening,” in which nude photos of dozens of female celebrities, some minors, were leaked online without the women’s consent).¹⁴ Nor does it touch upon the widespread harassment of women online, such as the “Gamergate” controversy, in which a number of explicit threats (both on and offline) were made against Anita Sarkeesian and other cultural critics who highlighted sexism in video game culture.¹⁵ The legal and social challenges presented by viral, distributed sexism of this nature are sufficiently distinct from the issues I discuss here that I do not attempt to include them in my analysis.

Finally, though this article does address nonconsensual and abusive sexual activity to some extent—particularly in the context of domestic violence and electronic monitoring or stalking of one’s (current or former) partner—it does not address rape specifically, or the relationship between technology and sexual violence more broadly. This is obviously an issue of pressing concern, but also one deserving of its own analysis, which I do not undertake here.¹⁶

III. THE LIFE COURSE OF INTIMATE SURVEILLANCE

Opportunities for the monitoring, recording, and quantification of intimate activity exist across a wide variety of intimate relations, behaviors, and activities. In this section, I outline a (non-exhaustive) list of some of the products and services available for intimate monitoring. I organize these practices roughly along the “life course” of a relationship—from the search for an intimate partner via dating, to consensual sexual behavior, to questions of fertility, to issues dealing with abuse, violence, and revenge.

11. Mark Latonero, *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*, TECH. & HUMAN TRAFFICKING, Nov. 2012, available at https://technologyandtrafficking.usc.edu/files/2012/11/HumanTrafficking2012_Nov12.pdf.

12. Neal Ungerleider, *How Mobile Phones and The Internet Fight (And Help) Human Trafficking*, CO.EXIST (Jan. 8, 2013, 2:44 PM), <http://www.fastcoexist.com/1681155/how-mobile-phones-and-the-internet-fight-and-help-human-trafficking>.

13. *Why The Price of Commercial Sex is Falling*, THE ECONOMIST (Aug. 11, 2014, 11:50 PM), <http://www.economist.com/blogs/economist-explains/2014/08/economist-explains-7>.

14. Valeriya Safronova, *Jennifer Lawrence’s Strong Stance on Privacy*, N.Y. TIMES (Oct. 10, 2014), <http://www.nytimes.com/2014/10/10/fashion/jennifer-lawrences-strong-stance-on-privacy.html>.

15. Nick Wingfield, *Feminist Critics of Video Games Facing Threats in ‘GamerGate’ Campaign*, N.Y. TIMES (Oct. 15, 2014), <http://www.nytimes.com/2014/10/16/technology/gamergate-women-video-game-threats-anita-sarkeesian.html>.

16. For an analysis of one aspect of the nexus between data collection and sexual violence, see Karen Levy, *Rape Is Not a Data Problem*, THE ATLANTIC (Oct. 30, 2014, 6:15 AM), <http://www.theatlantic.com/technology/archive/2014/10/rape-is-not-a-data-problem/381904/>.

A. Dating: Scoping Out Potential Intimates

The beginnings of intimate relationships are increasingly marked by their reliance on data collection about a potential partner. A good deal of this interpersonal surveillance occurs on standard social networks—it has become *pro forma* to investigate a potential mate through Google search and through monitoring his or her social media profiles (what’s commonly, and problematically, known as “Facebook stalking”).¹⁷ A wealth of articles in the popular press impart advice for covert yet effective monitoring via social media. As a representative *Cosmopolitan* column reports, “everyone’s lurked on someone’s Facebook page because they’ve hooked up with the person, or *want* to hook up with the person, or want to see the *last* person the stalkee has hooked up with.”¹⁸ The column continues to give readers tips about how to “stalk” without being detected (“unlike” something immediately if you accidentally “like” it; don’t reveal offline that you know lots of details about that person’s life history).¹⁹

In addition, a wealth of more specialized services offer the opportunity to gather and create data for use in budding romantic relationships. An app called Lulu²⁰ attracted enormous attention (and concern) when it was released as a “girls-only app for dating intelligence.”²¹ Lulu focuses on college campuses, and allows young women to anonymously review male friends, using a multiple-choice quiz (categories include “humor, manners, ambition, commitment level, look and style, sex and kissing”²²) and a selection of hashtags from a pre-populated list (#DudeCanCook, for instance, or #SexualPanther).²³ Lulu translates user input into a numerical rating visible to other users of the app.²⁴ (While previous versions of the app allowed women to rate any male associate to whom they were connected on Facebook, concerns about privacy and abuse led to a change in this policy such that men can only be reviewed and scored if they have explicitly opted into the service.²⁵)

Some services combine elements of online dating with data about a user’s geographic location, often to the chagrin of privacy advocates.²⁶ Apps like iHookup,²⁷ Tinder,²⁸ and Grindr²⁹ use mobile phones’ locative capabilities to match users with

17. See Marwick, *supra* note 8, at 387–88.

18. Dara Adeeyo, *9 Soul-Crushing Facebook Stalking Fails Everyone Makes*, COSMOPOLITAN (Sep. 13, 2013, 1:20 PM), <http://www.cosmopolitan.com/sex-love/advice/a4782/facebook-stalking-fails/>.

19. *Id.*

20. Lulu, <http://www.onlulu.com> (last visited May 11, 2015).

21. Mike Butcher, *Lulu Raises Another \$2.5M From Yuri Milner And Angels For Its Girls-Only App to Rate Guys*, TECHCRUNCH (Feb. 5, 2013), <http://techcrunch.com/2013/02/05/lulu-raises-another-2-5m-from-yuri-milnerangels-for-its-girls-only-app-to-rate-guys/>.

22. *What Is My Lulu Score?*, LULU, http://support.onlulu.com/knowledge_base/topics/what-is-my-lulu-score (last visited May 10, 2015).

23. Karen Levy, *Data-Driven Dating: How Data Are Shaping Our Most Intimate Personal Relationships*, PRIVACY PERSPECTIVES (Dec. 17, 2013), <https://privacyassociation.org/news/a/data-driven-dating-how-data-are-shaping-our-most-intimate-personal-relation>.

24. *Id.*

25. EJ Dickson, *Lulu Quietly Changed Its App So That It’s Opt-In for Dudes*, THE DAILY DOT (Mar. 19, 2014, 12:36 PM), <http://www.dailydot.com/technology/lulu-app-ranking/>.

26. See, e.g., *Locational Privacy*, ELECTRONIC FRONTIER FOUNDATION, <https://www.eff.org/issues/location-privacy> (last visited May 10, 2015).

27. *iHookup Social*, <http://www.ihookupsocial.com/> (last visited May 10, 2015).

28. *Tinder*, <http://www.gotinder.com> (last visited May 10, 2015).

others in their immediate proximity for opportune social or sexual encounters. Others cater to users with geographically particular concerns, such as an app developed in Iceland—a small country with a fairly homogeneous genetic pool—that draws on a large genealogical database to alert users with an “Incest Spoiler” if two mutually interested users share a common grandparent.³⁰

B. Tracking Intimate and Romantic Practices

Another set of services and applications facilitates “data-fication” of romantic or sexual behavior. One such app, *Spreadsheets*,³¹ captures audio and motion data using the iPhone’s microphone and accelerometer functionalities in order to track sexual performance. *Spreadsheets* graphs duration, number of thrusts, and audio volume, and allows users to set personal goals and “unlock” achievements.³² A number of similar apps are available, and often include the capability to keep records of several types of data (including, commonly, number and identity of sex partners, or duration and quality of sexual experiences).³³ The app *Hula* (recently rechristened as *Healthvana*)³⁴ takes another tack: it allows users to receive, verify, and share results of STD tests with sexual partners (through a process it calls “un-zipping”).³⁵

Wearable sex trackers are another breed of technologies in this space. The *SexFit* is a Wifi-enabled ring that sits at the base of the penis (currently in prototype stage) that tracks thrusting rhythm, speed, and calorie burn; the associated iPhone app “tells you whether to slow down or speed up your thrusting.”³⁶ In addition, “the *SexFit* allows the most dedicated users to share and compare their favourite sessions and impressive individual milestones with their peers on social media.”³⁷ The *kGoal*,³⁸ a “smart” pelvic floor exerciser, consists of a Kegel training tool wirelessly connected to a phone app; it visualizes progress and gives real-time biofeedback, and the company is reportedly at work on creating games to go along with the system.³⁹

A related group of technologies aims to gamify intimate relationships by incentivizing romantic behaviors through points, badges, levels, or other indicia of

29. *Grindr*, <http://grindr.com> (last visited May 10, 2015).

30. Ian Steadman, *App to Prevent ‘Accidental Incest’ Proves a Hit with Icelanders*, WIRED UK (Apr. 18, 2013), <http://www.wired.co.uk/news/archive/2013-04/18/iceland-incest-app>.

31. *Spreadsheets*, <http://spreadsheetsapp.com> (last visited May 10, 2015).

32. Eric Ravenscraft, *Spreadsheets Adds Data Tracking, Achievements to Your Sex Life*, LIFEHACKER (Mar. 14, 2014), <http://afterhours.lifehacker.com/spreadsheets-adds-data-tracking-achievements-to-your-s-1544181748>.

33. Deborah Lupton, *Quantified Sex: A Critical Analysis of Sexual and Reproductive Self-Tracking Using Apps*, 17 CULTURE, HEALTH & SEXUALITY (forthcoming 2015), available at <http://www.tandfonline.com/doi/full/10.1080/13691058.2014.920528#.U56zWfmSySo>.

34. *Hula*, <http://www.hulahq.com> (last visited May 10, 2015).

35. Eliana Dockterman, *STD Tests: There’s an App for That*, TIME, Jan. 7, 2014, available at <http://healthland.time.com/2014/01/07/std-tests-theres-an-app-for-that/>.

36. Editorial Staff, *New ‘Fitbit’ For Your Penis Tracks How Well You Have Sex*, NEXTSHARK, Aug. 7, 2014, <http://nextshark.com/new-fitbit-for-your-penis-tracks-how-well-you-have-sex/>.

37. *Id.*

38. MINNA LIFE, <http://www.minnalife.com/products/kgoal> (last visited May 10, 2015).

39. Daniel Cooper, *A Piece about a Smart Pelvic Floor Exerciser, Written by Someone Totally Out of Their Depth*, ENGADGET (Jun. 30, 2014, 5:18 AM), <http://www.engadget.com/2014/06/30/kgoal-pelvic-floor-exerciser-kickstarter/>.

success.⁴⁰ The (recently defunct) app Kahnoodle was one such example: its features included “sending push notifications to initiate sex; ‘Koupons’ that entitle the bearer to redeemable movie nights and kinky sex; and . . . [a] love tank, which fills or empties depending on how many acts of love you’ve logged.”⁴¹ Apps like this accord with calls from some researchers and clinicians for numerical marriage rating as a productive psychotherapeutic practice for couples.⁴²

C. Monitoring Fertility

Another class of technologies provide monitoring related to fertility and birth control. Data tracking related to fertility is not new: women have long tracked personal data (including menstrual cycle, basal body temperature, and other indicators) in order to facilitate or prevent pregnancy.⁴³ However, new services introduce a new dimension to such monitoring by embedding it more directly in women’s relationships—both intimate and commercial.

The app Glow,⁴⁴ launched in 2013 by PayPal founder Max Levchin, is credited by some as “[getting] 25,000 women pregnant.”⁴⁵ The app tracks a variety of types of data—menstruation, the position and firmness of a woman’s cervix, sexual intercourse (including the woman’s position during ejaculation), mood, and more—in order to predict ovulation.⁴⁶ For women who are already pregnant, the related app Glow Nurture⁴⁷ allows women to track pregnancy symptoms, and encourages healthy behaviors like exercise and taking prenatal vitamins.⁴⁸

But what distinguishes Glow and Glow Nurture from other fertility and pregnancy trackers (of which there are a number available) is that they explicitly make intimate data collection a family affair. Glow encourages you to sign up your partner to download a “mirror” app; the partner is prompted to provide additional data (for instance, to “provide ‘objective’ readings of your disposition”⁴⁹) and to respond to his partner’s cycle in certain ways—for instance, to send a “thoughtful

40. See generally JANE MCGONIGAL, *REALITY IS BROKEN: WHY GAMES MAKE US BETTER AND HOW THEY CAN CHANGE THE WORLD* (2011).

41. Susie Neilson, *When a Relationship Becomes a Game*, THE ATLANTIC (Aug. 8, 2013, 9:00 AM) <http://www.theatlantic.com/health/archive/2013/08/when-a-relationship-becomes-a-game/278459/>.

42. Elizabeth Bernstein, *Why Rate Your Marriage? A Numerical Score Can Help Couples Talk About Problems*, WALL ST. J. (Dec. 2, 2013, 7:10 PM) <http://www.wsj.com/articles/SB10001424052702304854804579234103858173602>.

43. Arielle Duhaime-Ross, *Apple Promised An Expansive Health App, So Why Can't I Track Menstruation?*, THE VERGE (Sept. 25, 2014, 12:55 PM), <http://www.theverge.com/2014/9/25/6844021/apple-promised-an-expansive-health-app-so-why-cant-i-track>.

44. GLOW, <https://glowing.com> (last visited Mar. 6, 2015).

45. Preetisha Sen, *How Max Levchin's Glow App Got 25,000 Women Pregnant*, FORTUNE (Aug. 27, 2014, 10:50 AM), <http://fortune.com/2014/08/27/how-max-levchins-glow-app-got-25000-women-pregnant/>.

46. GLOW, *supra* note 44.

47. GLOW NURTURE, https://glowing.com/features_nurture (last visited May 6, 2015).

48. *Id.*

49. Florence Williams, *Max Levchin Wants to Get You Pregnant*, SLATE (Jun. 20, 2013, 1:21 PM), http://www.slate.com/articles/double_x/doublex/2013/06/glow_fertility_app_max_levchin_will_pay_if_you_don_t_get_pregnant.html.

love text”⁵⁰ to a partner experiencing PMS. Glow also offers customized “tips” to both female users and their partners: “the app might remind a woman on an especially fertile day that it’s a good time to wear nice underwear. Her partner might receive a notification on the same day to bring flowers home.”⁵¹ The Glow Nurture app, for women who are pregnant, prompts a man to bring a glass of water to his partner if she has not yet logged eight glasses of water consumed via her own version of the app.

Glow doesn’t stop with partner integration. The company recently announced a new pharmacy partnership: if a woman tells Glow that she uses prescription birth control pills, Glow will remind her within the application when her prescription is running low, and will prompt her to refill the prescription at a Walgreens or Duane Reade.⁵² Integration with Walgreens’ Prescription Refill API allows her to authorize the refill directly within the app.⁵³

Another approach to fertility tracking is a group of period trackers intended to be used *by men*: a set of apps that track a woman’s menstrual cycle for the benefit of her partner’s ability to “manage” his relationship with her around it. The (now defunct) app PMSBuddy, which at one point boasted over 150,000 registered users,⁵⁴ offered “push notifications of upcoming PMS and the . . . ability to locate flower shops near you (via GPS).”⁵⁵ PMSTracker provided a similar service for the man “[t]ired of [his] wife/girlfriend/sister/mom/secretary biting [his] head off unexpectedly once a month.”⁵⁶ A man using the app Code Red⁵⁷ entered the last known day of his partner’s period into the app, and then waited to receive various push alerts (such as a “Horny Alert” which informs him he’s “able to score,” “Ovulation Alert”—time to “sit on the sidelines (unless you’re ready to start a junior league)” —and “Code Red Alert” for when “it’s game time and you’re way out of bounds.”⁵⁸ Finally, the (still available!) app iAmAMan not only enables period tracking, but assists in “private life planning”⁵⁹ by enabling tracking of several women’s cycles at once; but “[j]ust in case one of your ‘girlfriends asks you to

50. *Id.*

51. Lauren Goode, *Max Levchin’s New Plan: To Get You Pregnant (And Improve Health Care in the Process)*, ALL THINGS D (May 29, 2013, 11:14 AM), <http://allthingsd.com/20130529/max-levchins-new-plan-to-get-you-pregnant-and-improve-health-care-in-the-process/>.

52. *Refill Your Birth Control Prescription with Walgreens on Glow*, GLOW BLOG (Jan. 29, 2015), <http://blog.glowing.com/post/109494619045/refill-your-birth-control-prescription-with>.

53. Todd Wasserman, *Walgreens Now Lets Women Refill Birth Control Prescriptions Via Smartphones*, MASHABLE (Jan. 29, 2015), <http://mashable.com/2015/01/29/walgreens-birth-control-glow-app>.

54. Elinor Mills, *Menstrual Calendar Apps...For Men*, CNET (Feb. 3, 2009, 2:42 PM), <http://www.cnet.com/news/menstrual-calendar-apps-for-men/>.

55. Leena Rao, *PMSBuddy Helps (Men) Track That “Time of the Month,”* TECHCRUNCH (Feb. 19, 2010), <http://techcrunch.com/2010/02/19/pmsbuddy-helps-men-track-that-time-of-the-month/>.

56. Mills, *supra* note 54.

57. Monica Hesse, *‘Code Red’: iPhone/iPad App for Men Who Need to Track Women’s Menstrual Cycles*, WASHINGTON POST (Apr. 22, 2010), <http://www.washingtonpost.com/wp-dyn/content/article/2010/04/21/AR2010042104578.html>.

58. Jodi Jacobson, *iPhone, iPad Apps Allow Men to Track Women’s Menstrual Periods. Seriously.*, RH REALITY CHECK (Apr. 22, 2010, 8:00 AM), <http://rhrealitycheck.org/article/2010/04/22/iphone-apps-allow-track-womens-menstrual-periods-seriously/>.

59. Matt Buchanan, *IAmAMan Period-Tracking iPhone App for Sleazy, Shameless “Players,”* GIZMODO (Dec. 30, 2008 10:45 AM), <http://gizmodo.com/5120556/iamaman-period-tracking-iphone-app-for-sleazy-shameless-players>.

open up the app . . . each girl can be set with their [*sic*] own separate password, so when you punch it in, it only looks like you're tracking her."⁶⁰

D. Surveillance, Abuse, and Revenge

Monitoring technologies pervade a darker side of intimate relations, too—namely, keeping tabs on a partner's whereabouts and communications, often surreptitiously. These uses of data facilitate abusive relationships and electronic stalking, and are often used in situations involving domestic violence. In other situations, nonconsensual data “reveals” are used for retaliatory purposes—to exact “revenge” at the end of a relationship.

A huge number of partner “spy” apps exist, with names like Flexispy, Wife Spy, Girlfriend Spy, Spyera, and ePhoneTracker. The apps are intended to be installed surreptitiously on a partner's mobile phone, where they run undetected in “stealth mode”; they typically capture a wide range of information, generally including web browsing, phone call and messaging history (sometimes including audio recording), as well as real-time locational data.⁶¹ Some allow remote activation of the phone's microphone to unwittingly listen in on a partner by capturing ambient audio data.⁶² While some depend on an abuser temporarily taking physical control of the phone to install the application, others work differently. For instance, the now-defunct Loverspy was delivered through an electronic greeting card, which (after it was unwittingly opened by a victim) installed malware that was used to capture the content of messages, passwords, and web history; the FBI has since indicted Loverspy's creators.⁶³

The marketing of such applications can be shocking. HelloSpy, which intercepts phone location as well as contacts, app usage, web history, and the content of messages, advertises that “[t]he past two decades has [*sic*] made infidelity more accessible than ever mostly because of the ascent of two majorly disruptive technologies: online social networks and mobile phones. Up to 90% of marital affairs may include the use of a mobile phone or email as a preferred means for communication.”⁶⁴ This information appears alongside a photograph of a man physically restraining a woman, whose face is visibly beaten and lacerated.⁶⁵ This disturbing “testimonial” appears to suggest that the man was able to detect, and fittingly punish, his partner's infidelity thanks to the services of HelloSpy.

Domestic violence advocacy groups say that the use of such apps has reached “epidemic proportions”; one study estimates that over 50 percent of abusive part-

60. *Id.*

61. Cahal Milmo, *Exclusive: Abusers Using Spyware Apps to Monitor Partners Reaches 'Epidemic Proportions'*, THE INDEP. (Dec. 26, 2014), <http://www.independent.co.uk/news/uk/home-news/exclusive-abusers-using-spyware-apps-to-monitor-partners-reaches-epidemic-proportions-9945881.html>.

62. *Id.*

63. Lisa Vaas, *FBI Seeking "Loverspy" Hacker Who Helped Jealous Lovers Plant Spyware*, NAKED SECURITY (Nov. 8, 2013), <https://nakedsecurity.sophos.com/2013/11/08/fbi-seeking-loverspy-hacker-who-helped-jealous-lovers-plant-spyware>.

64. *Cheating by the numbers . . .*, HELLOSPY, <http://hellospy.com/hellospy-for-personal-catch-cheating-spouses.aspx> (last visited Feb. 11, 2015).

65. *Id.*

ners use “some . . . form of electronic surveillance to stalk their victims.”⁶⁶ In another survey, 85% of domestic violence shelters said they worked with victims who were stalked using GPS, and women are advised to complete a “digital detox” upon intake to prevent abusers from locating them at the shelter.⁶⁷

It should be noted that not all abuse and harassment using digital data depend on specialized cyberstalking apps. “Real name” policies on some web services can facilitate continued abuse of victims,⁶⁸ as can data brokers and websites that catalogue contact information and residential history.⁶⁹

Finally, intimate data are often revealed non-consensually for retaliatory purposes. The best-known exemplar is what’s often called “revenge porn,” in which sexually explicit photographs of one partner are posted or distributed online without that partner’s consent. In other cases, revenge-seeking partners may post incriminating evidence of adultery to social media (e.g., text messages).⁷⁰

IV. RISKS AND IMPLICATIONS

Should it come as a surprise that intimate relationships are increasingly governed by monitoring and quantification? Not particularly. As described, data’s infiltration of intimacy follows its intrusion into virtually every other social sphere. But the rise of data in intimate relations poses unique risks to privacy and challenges to interpersonal dynamics, which I outline here.

A. Quantification as Objectivity, Measurement as Control

It’s entirely understandable that there’s a market for intimate surveillance and quantification. These technologies purport to give users more control and knowledge in an area of life rife with unknowns and in which users are uniquely vulnerable, both emotionally and physically. Just as we aim to reduce uncertainty in our consumer lives by reading Yelp reviews—or by checking up on the whereabouts of our packages using online shipment trackers—we similarly try to protect our interests and grant ourselves a modicum of control by screening and tracking information about our intimate relations and behaviors.

But the act of measurement is not neutral. Every technology of measurement and classification legitimates certain forms of knowledge and experience, while rendering others invisible.⁷¹ The types of data that are tracked and measured by

66. Milmo, *supra* note 61.

67. Aarti Shahani, *Smartphones Are Used to Stalk, Control Domestic Abuse Victims*, NPR ALL TECH CONSIDERED (Sep. 15, 2014, 4:22 PM), <http://www.npr.org/blogs/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims>.

68. Karyne Levy, *Drag Queens Aren’t the Only People Affected by Facebook’s ‘Real Name’ Policy*, BUSINESS INSIDER (Sept. 24, 2014, 8:02 PM), <http://www.businessinsider.com/drag-queens-arent-the-only-people-affected-by-facebooks-real-name-policy-2014-9>.

69. Jim Adler, *TrueRep: Why It’s Important*, JIM ADLER BLOG (Dec. 2, 2011), <http://jimadler.me/post/13438945247/truerep-why-its-important>.

70. See, e.g., Jordan Sargent, *NFL Player Tweets Racy Texts Between Wife and Dallas Cowboys Superstar*, GAWKER (Dec. 4, 2014, 9:54 PM), <http://gawker.com/nfl-player-reveals-racy-texts-between-wife-and-dallas-c-1667060864>.

71. See generally GEOFFREY C. BOWKER & SUSAN LEIGH STAR, SORTING THINGS OUT: CLASSIFICATION AND ITS CONSEQUENCES (2000).

these apps are embedded in technological contexts, as well as sociocultural contexts. For instance, for sex tracker apps, most smartphones are capable of tracking audio and accelerometer data, so these types of data are what get counted (and constructed as “good” sexual behaviors): “sex is judged by thrusting, success is judged by endurance, and pleasure is measured in moans.”⁷² Because these technologies generate numbers that can be charted, graphed, and compared to the “performance” of others, they simplify highly personal and subjective experiences to commensurable data points, and run the risk of reductively (and normatively) constructing the “quality” of intimate behaviors along a very limited set of axes.⁷³ As described by Lupton, such technologies thus introduce an “algorithmic subjectivity” to our understandings of intimate relations and behaviors.⁷⁴

These devices could . . . be regarded as disciplinary, working to tame the sexual and reproductive body by rendering it amenable to monitoring, tracking, and detailed analysis of the data thus generated[. . . .] These technologies configure a certain type of approach to understanding and experiencing one’s body, an algorithmic subjectivity, in which the body and its health states, functions and activities are portrayed and understood predominantly via quantified calculations, predictions and comparisons.⁷⁵

The ways we regulate and police intimate technologies are also not neutral, but governed by the sociocultural realities in which we live. Consider Sarah Jeong’s contention that law enforcement is often complicit “in the abuse of technology”⁷⁶ related to intimate violence, in part because law enforcement officers are overwhelmingly male, and in part because intrusions on intimate data (including sexual images) have become disturbingly routine “perks” in law enforcement contexts, from the NSA to the California Highway Patrol.⁷⁷ Further, it is striking how many technologies of intimate surveillance construct women, in particular, as monitored subjects. From women’s bodies and cycles to their whereabouts, communications, and activities, services from Glow to Wife Spy to Girls Around Me expose women especially to data collection, invasive monitoring, and increased visibility.

Intimate surveillance gives us a sense of control over a fundamentally uncontrollable dimension of personal life: we can only control that which we can track and measure.⁷⁸ As Foucault states, “power will be exercised by virtue of the mere fact of things being known and people seen[.]”⁷⁹ But this sense of control can, ultimately, be illusory—and the impulse can be quite harmful to intimate relations (or in some situations, even criminal and pathological).

72. Rose Eveleth, *How Self-Tracking Apps Exclude Women*, THE ATLANTIC (Dec. 15, 2014, 7:01 AM), <http://www.theatlantic.com/technology/archive/2014/12/how-self-tracking-apps-exclude-women/383673>.

73. Lupton, *supra* note 33.

74. *Id.* at 10.

75. *Id.*

76. Sarah Jeong, *Surveillance Begins At Home*, FORBES (Oct. 28, 2014, 4:31 PM), <http://www.forbes.com/sites/sarahjeong/2014/10/28/surveillance-begins-at-home>.

77. *Id.*

78. See generally JAMES C. SCOTT, *SEEING LIKE A STATE: HOW CERTAIN SCHEMES TO IMPROVE THE HUMAN CONDITION HAVE FAILED* (1998); MICHEL FOUCAULT, *POWER/KNOWLEDGE: SELECTED INTERVIEWS & OTHER WRITINGS, 1972-1977* (1980).

79. FOUCAULT, *supra* note 78, at 154.

B. Monitoring, Trust, and Intimate Values

As intimate data-gathering becomes more prevalent, the reality of social surveillance becomes increasingly normalized—in both intimate and non-intimate contexts. The more we encounter and use such technologies, the more they come to be seen as simply a fact of modern relational life, and an inescapable component of intimacy.⁸⁰ Consider how normal (and normative) the “Facebook stalk” and other means of gathering pre-dating intelligence have already become; at minimum, Googling a potential partner before dating him or her is essentially social due diligence. We might expect to see other areas of intimate life become increasingly governed by such a surveillant paradigm.

A data-driven mentality might affect the qualities of intimate relations as well.⁸¹ Digital records create new sites of accountability that appear morally neutral and can come to displace social trust. Trust has long been an essential foundation of intimate relations and an important motivator of prosocial behavior. If partners remain faithful because they’re afraid of being “tattled on” by digital technology, rather than out of a sense of loyalty to their partner, does fidelity retain its longstanding social and emotional significance?

Similarly, apps that quantify or calculate previously incommensurable aspects of intimate relationships may create new motivations for certain behaviors. For instance, regarding Kahnoodle and other romance quantifiers, psychologist Eli Finkel suggests that gamification may foster a tit-for-tat “exchange mentality” that is ultimately detrimental to the foundations of intimate relations, and ultimately divests romantic gestures of their meaning.⁸²

C. Privacy Risks

Increased data collection brings with it increased risk to privacy, as data are put to unanticipated uses, security safeguards are breached, or information flows to commercial parties who are external to the immediate intimate relation. A number of discrete risks exist; some stem primarily from the parties to the relationship themselves, while others relate to the commercial technological platforms on which intimate monitoring typically relies.

Some of the sorts of monitoring described here are (or could easily be used in ways that are) surreptitious or nonconsensual. Sex trackers don’t require the consent of the other party before data about that party is entered. Apps that facilitate digital stalking are, essentially by definition, nonconsensual, as is the posting of revenge porn. Some dating data collectors draw on users’ location without their explicit consent; for instance, for a period of time, an iPhone app called Girls Around Me drew on women’s publicly visible Facebook and Foursquare data to

80. See Levy, *supra* note 6, at 79 (“Relational data practices may instill in the public a tolerance for watching and being watched, measuring and being measured, that leads us to abide additional surveillance without much complaint.”).

81. Levy, *supra* note 23.

82. Neilson, *supra* note 41.

create a real-time “radar map,” complete with photos, of women around the user.⁸³ (The app was later pulled from the iTunes Store.)⁸⁴

A second set of privacy risks relates to the fact that intimate data are typically collected by, and stored on, decidedly non-intimate commercial platforms. Thus, even data that appear to be shared only within an intimate partnership may also be shared with (or sold to) other parties—including app developers, internet service providers, advertisers, or data brokers and aggregators.⁸⁵ These relationships are typically governed by fine-print privacy policies and terms-of-service agreements—but we know that consumers very rarely read and understand such agreements,⁸⁶ that the way they are presented often makes consumers vulnerable to exploitation,⁸⁷ and that, under the third-party doctrine, the “voluntary” revelation of data to third parties reduces the reasonable expectation of privacy that legally inheres in such data for purposes of Fourth Amendment protection.⁸⁸

Sometimes the revelation of intimate data by commercial actors seems to be unintentional. In 2011, Fitbit (a wearable pedometer with associated activity tracker app) received negative press for a gaffe in which it revealed intimate data about users’ sexual practices, apparently inadvertently.⁸⁹ Fitbit users’ profiles, including activity tracking information users had manually inputted into the app, were set to be public by default; among the categories of activity users could report were “sexual activity – active, vigorous effort” and “sexual activity – passive, light effort, kissing, hugging,” along with the duration of such activity.⁹⁰ Not only were these data made public, and associated with users’ identifying information on Fitbit’s site (at least, until Fitbit realized its gaffe and changed its settings),⁹¹ but the infor-

83. John Brownlee, *This Creepy App Isn’t Just Stalking Women Without Their Knowledge, It’s A Wake-Up Call About Facebook Privacy*, CULT OF MAC (Mar. 30, 2012, 3:20 PM), <http://www.cultofmac.com/157641/this-creepy-app-isnt-just-stalking-women-without-their-knowledge-its-a-wake-up-call-about-facebook-privacy/>.

84. John Brownlee, *Creepy Girl-Stalking App Girls Around Me Has Been Yanked From The App Store*, CULT OF MAC (Mar. 31, 2012, 7:29 PM), <http://www.cultofmac.com/157918/creepy-girl-stalking-app-girls-around-me-has-been-yanked-from-the-app-store/>.

85. Christian Payne, *How Activity Trackers Remove Our Rights to Our Most Intimate Data*, GUARDIAN (Jun. 3, 2014, 7:11 AM), <http://www.theguardian.com/technology/2014/jun/03/how-activity-trackers-remove-rights-personal-data>.

86. Yannis Bakos et al., *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1 (2014).

87. Florencia Marotta-Wurgler, *Some Realities of Online Contracting*, 19 SUP. CT. ECON. REV. 11 (2011).

88. *Smith v. Maryland*, 442 U.S. 735, 745 (1979). In this digital age, the days of the third-party doctrine may be numbered. *See U.S. v. Jones*, 132 S. Ct. 945, 957 (Sotomayor, J., concurring) (“it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.”).

89. Zee, *Fitbit Users Are Unwittingly Sharing Details of Their Sex Lives With The World*, THENEXTWEB (Jul. 3, 2011, 3:21 PM), <http://thenextweb.com/insider/2011/07/03/fitbit-users-are-inadvertently-sharing-details-of-their-sex-lives-with-the-world/>.

90. Jack Loftus, *Dear Fitbit Users, Kudos on the 30 Minutes of “Vigorous Sexual Activity” Last Night*, GIZMODO (Jul. 3, 2011, 1:25 PM), <http://gizmodo.com/5817784/dear-fitbit-users-kudos-on-the-30-minutes-of-vigorous-sexual-activity-last-night>.

91. Kashmir Hill, *Fitbit Moves Quickly After Users’ Sex Stats Exposed*, FORBES (Jul. 5, 2011, 7:58 AM), <http://www.forbes.com/sites/kashmirhill/2011/07/05/fitbit-moves-quickly-after-users-sex-stats-exposed/>.

mation was also indexed by Google; at one point, a journalist reported retrieving twelve pages of search results for users' intimate data.⁹²

Recall that the fertility app Glow gathers such fine-grained and sensitive data as emotional mood, a woman's position when her partner ejaculates, the firmness of her cervix, and quite a bit more—and explicitly encourages a female user to connect with her partner using the app.⁹³ Recall as well that Glow has recently partnered with Walgreens pharmacies to facilitate in-app purchase of users' birth control prescriptions there.⁹⁴ But what is less apparent from Glow's interface is the extent to which users' data may be put to other uses. For one, Glow aims to collect and aggregate enough data about its users' fertility that it can possibly spot as-yet-unknown correlations for medical study.⁹⁵ Max Levchin, the app's founder, jokes that “[i]t would be awesome if we could be partly responsible for finding a cure for infertility.”⁹⁶

In addition, Glow is aiming to bring its big data to bear on the health insurance market. According to a recent *Venturebeat* report, Glow's co-founder and CEO Mike Huang suggested that using Glow's data to achieve “a more granular understanding” of health could provide “more accurate risk assessments ... ultimately result[ing] in better health insurance.”⁹⁷ It is not clear what “better” means in this instance, or for whom better outcomes are expected to result.

Though Glow may very well take steps to preserve individual users' privacy in putting their data to such uses—for instance, by aggregating the data or scrubbing it of personally identifiable information before analyzing it or sharing it with other parties—contemporary understandings of privacy suggest that such practices may still be normatively problematic, in that they are unlikely to accord with users' expectations about the use of their sensitive data⁹⁸ or the ecosystems through which such information flows (in other words, such uses are likely to violate what Helen Nissenbaum terms the contextual integrity⁹⁹ of these intimate information flows).

Security breaches are a third area of significant threat, especially in light of the acutely sensitive nature of intimate data. Security researchers recently identified a technical flaw in Grindr (a mobile dating app used primarily by gay men) that enabled real-time, pinpoint location tracking of any one of its users.¹⁰⁰ After the researchers notified Grindr of the problem—and after Egyptian authorities report-

92. Loftus, *supra* note 90.

93. See Williams, *supra* note 49.

94. See Wasserman, *supra* note 53.

95. Farhad Manjoo, *Glow vs. Stick*, SLATE (Aug. 8, 2013, 11:00 AM), http://www.slate.com/articles/technology/technology/2013/08/new_fertility_app_glow_it_wants_to_know_absolutely_everything_about_you.single.html.

96. *Id.*

97. Kia Kokalitcheva, *Glow Brings in \$17M in New Funding, Puts Big Data to Work For Women's Health*, VENTUREBEAT (Oct. 2, 2014, 6:00 AM), <http://venturebeat.com/2014/10/02/glow-brings-in-17m-in-new-funding-as-puts-big-data-to-task-with-fertility-challenges/>.

98. See Lupton, *supra* note 33, at 13 (“Until very recently, many mobile app users viewed the information stored on their apps to be private, not realising the extent to which the app developers used these data for their own purposes”).

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

100. Dan Goodin, *How Dating App Grindr Makes It Easy to Stalk 5 Million Gay Men*, ARS TECHNICA (Jan. 16, 2015, 2:22 PM), <http://arstechnica.com/security/2015/01/how-dating-app-grindr-makes-it-easy-to-stalk-5-million-gay-men/>.

edly used Grindr to track down gays and prosecute them for illegal homosexual conduct (though it is unclear if the authorities exploited this particular weakness in doing so)¹⁰¹—Grindr disabled location tracking in several countries with anti-gay laws. However, the weakness appears to persist in other countries, and seems to be common across location-based dating apps.¹⁰²

V. CONCLUSION

As a final inquiry, we should also ask how law and policy will approach intimate data-gathering. Law is making inroads, albeit slowly, in some of these contexts, particularly in cases in which data use intersects with criminal law or clear cases of nonconsent. Senator Al Franken has repeatedly introduced the Location Privacy Protection Act in Congress, which would forbid stalking apps from being developed or sold, and would make it more difficult to collect or share locational data without consent¹⁰³ (though app developers have been quick to “rebrand” as legal child or employee monitors in order to escape such regulation).¹⁰⁴ And a number of legal efforts to combat revenge porn have taken root, from criminal statutes¹⁰⁵ to dedicated law firm initiatives¹⁰⁶ to the use of copyright law.¹⁰⁷ But as a rule, law has been loath to get too involved in intimate domains (or to “rais[e] the curtain upon domestic privacy”¹⁰⁸ by exposing to “the evil of publicity”¹⁰⁹ that which “ought to be left to family government”),¹¹⁰ and some of the new sorts of privacy risks created by intimate surveillance are not easily addressable by existing legal frameworks (for instance, data-sharing practices that are technically permissible under terms-of-service agreements, but which violate user expectations and contextual norms).

Surveillance poses new challenges in intimate relational contexts. It encourages an “algorithmic subjectivity” about sexual behavior, normalizes monitoring practices and data-driven approaches to intimate relations, and brings to the fore complex and thorny issues around privacy, consumer expectations, and the integrity of information flows. This article is not intended to advocate for technological, Luddism, or fear-mongering in the face of increased data-gathering; rather, it aims

101. Rick Noack, *Could Using Gay Dating App Grindr Get You Arrested In Egypt?*, WASH. POST (Sep. 12, 2014), <http://www.washingtonpost.com/blogs/worldviews/wp/2014/09/12/could-using-gay-dating-app-grindr-get-you-arrested-in-egypt/>.

102. Goodin, *supra* note 100 (security researcher Colby Moore reports that he “looked at five or so dating apps and all are vulnerable to similar vulnerabilities”).

103. Aaron Rieke, *Use of Stalking Apps on the Rise, Advocates Report*, EQUAL FUTURE (Jan. 7, 2015), <http://equalfuture.us/2015/01/07/stalking-apps-on-the-rise/>.

104. Kashmir Hill, *How Smartphone Spyware Peddlers Pretend Their Apps Aren't Put to Illegal Use*, FORBES (Sep. 30, 2014, 7:59 PM), <http://www.forbes.com/sites/kashmirhill/2014/09/30/stealthgenieugly-marketing-of-spyware/>.

105. Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 371 (2014).

106. Matthew Goldstein, *Law Firm Finds Project to Fight 'Revenge Porn'*, N.Y. TIMES (Jan. 29, 2015, 7:47 PM), <http://dealbook.nytimes.com/2015/01/29/law-firm-finds-project-to-fight-revenge-porn/>.

107. See Amanda Levendowski, *Using Copyright to Combat Revenge Porn*, 3 N.Y.U. J. INTELL. PROP. & ENT. L. 422 (2014).

108. *State v. A.B. Rhodes*, 61 N.C. (Phil.) 453, 459 (1868).

109. *Id.* at 454.

110. *Id.*

to bring these emergent practices to light, so that we might consider their normative and social implications, as intimate relations become permeated by the data paradigm.