11-2023

Liking the Intrusion Analysis in *In Re Facebook*

Jane R. Bambauer

Jane R. Bambauer*

Liking the Intrusion Analysis in *In Re Facebook*

https://doi.org/10.1515/jtl-2023-0044
Received November 20, 2023; accepted November 20, 2023; published online March 25, 2024

Abstract: *In re Facebook* preserved a class action brought against Facebook based on its mass collection of web browsing data. Although the plaintiffs brought several common law and statutory causes of action, I will focus on the court's analysis of intrusion upon seclusion. This is where the case makes its greatest contribution to 21st century jurisprudence. It clears up several puzzles that had troubled the tort (and indeed my own thinking) to the great benefit of tort theory and the progress of privacy law.

Keywords: Intrusion Upon Seclusion; privacy; Internet Law; social media; Data Privacy; Facebook

1 Introduction

In re Facebook[1] preserved a class action brought against Facebook based on its mass collection of web browsing data. Although the plaintiffs brought several common law and statutory causes of action, I will focus on the court's analysis of Intrusion Upon Seclusion. This is where the case makes its greatest contribution to 21st century jurisprudence. It clears up several puzzles that had troubled the tort (and indeed my own thinking) to the great benefit of tort theory and the progress of privacy law.

Specifically, the case clarifies the enduring viability and wisdom of the Intrusion Upon Seclusion tort by recognizing that:

(a) The concept of "seclusion" is timeless and flexible enough to adapt to new technologies and environments;
(b) Intrusions therefore interfere with legally cognizable interests of the individual who is observed (and this is true even if the intrusion is facilitated by a third party who is permitted to observe the plaintiff); and

1 956 F.3d 589 (9th Cir. 2020).

***Corresponding author: Jane R. Bambauer**, University of Arizona James E. Rogers College of Law, Gainesville, FL, USA, E-mail: janebambauer@ufl.edu

(c) Nevertheless, intruders may engage in innocuous or socially beneficial pursuits. The "highly offensive" element protects *their* interests by incorporating them directly into the prima facie case

Given the soundness and flexibility of these principles (as illustrated by the facts and analysis from the case itself), *In re Facebook* forges a path for privacy law. It demonstrates not only the relevance of old torts to modern privacy debates but indeed their superiority.

2 The Case

The facts of the case get right at the routines that make the guts of the commercial Internet.

Every website that has a Facebook "like" button has made a deal with Facebook that is advantageous to both parties. If visitors to the website click the "like" button, the third-party website gets a boost in the number of followers and will have their content promoted more generously in Facebook's newsfeed algorithm.[2] Facebook, in turn, gets advantages for its business as an ad exchange. When a website imbeds the "like" button, they include HTML code that replicates a visitor's website retrieval requests and sends it to Facebook.[3] As a result, Facebook collects data on the URLs of every visitor to those websites. If a visitor has a Facebook account, then Facebook would have already placed small text files ("cookies") on the user's devices that would store the browsing histories of that account-holder.[4]

From the facts of the case it is not clear what the websites themselves disclosed to individuals who visited their websites. Privacy disclosures may have varied significantly over the field of third party websites. But Facebook's own privacy policies and end user agreements promised (or at least strongly implied) that Facebook would *not* collect browsing information for logged-out users.[5] In fact, Facebook *did* store the browsing information in their cookies even if the user was logged out of Facebook.[6]

2 "Clicking the LIKE button on the upper right-hand side of a Business Page serves two purposes. For a business, this is very important information to them, as it allows them to show the number of followers that they've gained utilizing social media, thereby tracking their Social Media ROI (Rate Of Influence). Secondly, although with Facebook's new algorithm it's not a guarantee, it most likely will boost the chance that you'll get updates, event notifications, and a deeper connection with that person or company." https://gosalesandmarketing.com/the-importance-of-the-facebook-like/.

3 In re Facebook, at 596.

4 Id.

5 Id. at 602.

6 Id.

The browsing history data was subsequently used to help Facebook in its targeted advertising business, as Facebook was able to attract more advertisers and command higher ad placement prices if it could promise the ad would reach a more relevant audience (that is, an audience more likely to click on the ad and make a purchase.[7])

These basic facts are simultaneously shocking and commonplace. They are shocking because in the course of human experience, it had never before been possible, let alone easy, to observe and collect so much detail about the attention and inner life of others. And it is commonplace because the predominant business model for Internet firms is a modern variant of the broadcast model: Internet companies offer elaborate and popular content and services for $0 price and fund their operations through behavioral advertising.

To the defenders of strong privacy rights, including those who brought or support the litigation in *In re Facebook,* the modern methods of behavioral advertising cross a line that should be recognized and fully protected in American law. The plaintiffs brought claims for breach of contract and technical violations of wiretap laws,[8] but the intrusion tort is the most important. It provides a source of legal protections that can apply across contexts when information-collection upsets expectations and offends norms. Unconsented observation where you would not expect it *does* cause harm. Even if the information is not misused, the observation and collection interferes with an individual's valid interests in controlling their information.[9]

At the same time, the case continues the American tradition of treating privacy as one of many objectives in a bustling zone of conflicting activities. In the U.S., interests in information-gathering are *also* presumptively valid and potentially socially useful. Unlike the rigid privacy protections recognized in Europe and to a lesser degree in states like California, *In re Facebook* interprets the intrusion tort to manage risks in context without creating sticky property-style rights. If we take seriously the court's entire analysis, the opinion raises serious doubts about whether the arrangement Facebook had with its users and third-party websites could support legal intervention *even if* all agree that its conduct was intrusive.

This commitment to treating privacy as part of the management of conflicting activities rather than as a fundamental right bestowed to data subjects is a virtue. It

7 Brett R. Gordon et al., *A Comparison of Approaches to Advertising Measurement: Evidence from Big Field Experiments at Facebook* (2018). The opinion says that Facebook creates behavioral profiles that are "sold to advertisers" (Id. at 596), but in fact, advertisers describe their target audience to Facebook without receiving any personal data. *See* https://www.facebook.com/business/ads/ad-targeting.

8 The court's analysis of the Wiretap Act is highly flawed, in my opinion, absent an allegation that Facebook had promised the third party websites that it would not collect data from Facebook users who were not logged in. *See* Pharmatrak. Without this allegation, the defendant's motion to dismiss should have been granted.

9 Jane Bambauer, The New Intrusion

will set the intrusion tort up for success as privacy law is forced to respond to new uses of personal data in AI, autonomous vehicles, health innovations, and other areas where meaningful systems of consent will be impractical or undesirable.

3 Seclusion Is a Timeless Concept

As a reminder, the Second Restatement defines Intrusion upon Seclusion as so:

§ 652B Intrusion Upon Seclusion One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

The analysis in *In re Facebook* started with a consideration of the "seclusion" element.[10] Courts often rely on the customary-but-vague concept of reasonable expectations of privacy, and this case is no different.[11] The trouble is, unlike norms that have developed in physical space, where property rules and architectural markers can create physical signs of expectations, norms are neither clear nor strong on new digital media.

Fortunately, Judge Thomas's opinion makes important strides. According to the opinion,

> *both* the nature of collection and the sensitivity of the collected information are important. The question is not necessarily whether Plaintiffs maintained a reasonable expectation of privacy in the information in and of itself. Rather, we must examine whether the data itself is sensitive *and* whether the manner it was collected – after users had logged out – violates social norms.[12]

This is a highly substantive and non-obvious contribution to civil privacy law. After all, under Fourth Amendment law, *only* the nature of collection matters. Police are free to collect and observe highly sensitive information as long as their conduct does not constitute a "search."[13] And conversely, if police conduct *is* a search, they will have violated Fourth Amendment reasonable expectations of privacy even if the

10 This could also be described as the "intrusion" element because whether the defendant "intruded", with the negative implications that term has, will depend on whether the defendant was making observations or gathering information in a context that would be considered the plaintiff's "seclusion."

11 "We first consider whether a defendant gained unwanted access to data by electronic or other covert means, in violation of the law or social norms. To make this determination, courts consider a variety of factors, including the customs, practices, and circumstances surrounding a defendant's particular activities. Thus, the relevant question here is whether a user would reasonably expect that Facebook would have access to the user's individual data after the user logged out of the application." Id. at 601–02.

12 Id. at 603.

13 Greenwood, 486 U.S. 35 (1988).

observations they made were trivial – observations of a serial number or a front porch, for example.[14] But these Fourth Amendment rules were developed when arguments were highly contingent on physical space. Given that *In re Facebook* concerns reasonable expectations where there is no long history of human customs and norms, Judge Thomas's decision to incorporate means *and* content of the information-gathering makes good sense.

On the matter of Facebook's means, two factors weighed heavily in Judge Thomas's opinion that Facebook may have intruded on users' seclusion. First, the data collection was "surreptitious and unseen,"[15] providing no visible or obvious notice that it was happening at the time. Second, Facebook's privacy policies made "affirmative statements that it would not receive information from third-party websites after users had logged out."[16] Thus, Facebook affirmatively encouraged an expectation among its users that they would not be tracked by Facebook if they were logged out of their accounts. "Facebook set an expectation that logged-out user data would not be collected, but then collected it anyway."[17]

As for the substance of the information that was gathered, the court said:

> The nature of the allegedly collected data is also important. Plaintiffs allege that Facebook obtained a comprehensive browsing history of an individual, no matter how sensitive the websites visited, and then correlated that history with the time of day and other user actions on the websites visited. … we conclude there remain material questions of fact as to whether a reasonable individual would find the information collected from the seven million websites that employ Facebook plug-ins "sensitive and confidential."[18]

Combining the sensitivity and the means of collection, the court found the plaintiffs had a strong enough showing on "seclusion" to overcome a summary judgment motion.

I agree with the court's method of analysis and conclusion, but also offer a small objection. On methods, the court's approach to looking at methods and sensitivity together is a positive development in privacy law for several reasons. First, it makes use of privacy policy statements without allowing them to dictate the entire case. A firm that promises it will not collect data and then collects it anyways is much more likely to be found to be violating their customer's seclusion, but possibly not if the information gathered is impersonal, already public, or a matter of common knowledge. And at the same time, if a firm says nothing in the privacy policy that would encourage an expectation of privacy or even affirmatively discloses that it intends to use a certain data-collection practice, that provision of notice will certainly

14 Arizona v. Hicks
15 In re Facebook at 603.
16 Id.
17 Id. at 602.
18 Id. at 603.

weigh in favor of the defendant but should not preclude an argument that the practice still intruded the customer's seclusion. Common sense dictates this should be so. If a Starbucks privacy policy states clearly that the company will collect saliva samples from your disposed coffee cups and run a DNA genotyping analysis, the fact that the practice was disclosed somewhere is not dispositive.

The only nit I have with Judge Thomas's analysis of "seclusion" concerns the sensitivity of the data that Facebook collected. The court accepted uncritically the plaintiffs' claim that Facebook collected data from third party websites "no matter how sensitive" those websites were. While a comprehensive browsing history collected by a browser, by a basic Internet service provider, or by a search engine may include information about a person's visits to sensitive websites, it's implausible that the most sensitive websites would decide to imbed a "like" button. Facebook users may have visited abortion websites or Web MD pages that describe the symptoms of gonorrhea, but there's little reason to assume those websites ask their visitors to "Like Us on Facebook!" This relates to a more general complaint I have with the opinion: throughout, the court does not give adequate consideration to the incentives that the third party websites would have to either coordinate with Facebook or, in the case of a highly sensitive website, to *avoid* imbedding a Facebook button. Thus, it could very well be that all seven million of the websites that imbedded the Facebook button are non-sensitive, at least when you consider each individually.

Nevertheless, this criticism is minor because the extended profile of web browsing that Facebook collected makes the collection as a whole more sensitive than any of its constituent parts.[19] In physical space, this theory was developed in the case Ralph Nader brought against GM based in part on their effort to tail him everywhere he went in public for an extended period of time.[20] Thus, given that the data as a whole is somewhat sensitive, and the methods were somewhat deceptive, it was fair to conclude the plaintiffs had raised enough evidence to at least make "seclusion" a triable issue.

4 Intrusions Interfere with an Individual's Valid Interests Even when the Intruders Have Help from Insiders

Having found that Facebook users may have expected their browsing histories to be part of their reasonably expected seclusion (and having provided some factors to help

19 This is the "mosaic effect." https://www.brookings.edu/research/databuse-digital-privacy-and-the-mosaic/, https://scholarship.law.bu.edu/faculty_scholarship/624/.

20 Nader v. General Motors Corp. – 25 N.Y.2d 560, 307 N.Y.S.2d 647, 255 N.E.2d 765 (1970).

future jurists and litigants understand what that means in digital space), it may be obvious that Facebook *intruded* on that seclusion by intentionally collecting the very information that was within its scope. Indeed, courts *should* treat "intrusion" and "seclusion" as the same element, determined by the same corpus of facts. Nevertheless, there are a couple additional details from the case that relate to intrusion and are worth elaborating. "Intrusion," with all the negative connotation the term brings with it, insists that the defendant has done something that negatively affects the plaintiff's interests. If the definition of "seclusion" were too broad – if it covered everything that could be known about a person including their name, their publicly posted comments, or their appearance in a public place – intrusions would be a constantly occurring phenomenon with ambiguous impact on the wellbeing of the individuals who are observed. But if "seclusion" is closely drawn – if it really is the conceptual equivalent to being in your own house with your blinds drawn – then the intrusion into that seclusion necessarily has a negative impact for the person observed.

This may seem obvious, but it is important to the Facebook case (and future privacy cases) for two reasons. First, it allows the court to easily overcome standing objections. Facebook had argued that the plaintiffs failed to allege a concrete harm under *Spokeo* and *Lujan.*[21] The court disagreed. The right to privacy, which has a long history in the U.S. common law,[22] encompasses an individual's reasonable expectations of control over their personal information.[23] Even if the plaintiffs' claim proves unsuccessful because of a failure to prove that the intrusion was highly offensive, an allegation that an intrusion into one's seclusion occurred at all is a sufficient injury to clear the standing hurdle.[24]

As is so often the case, an analogy to real property or bodily integrity is instructive.[25] An unconsented trespass or physical contact with the body may turn out to fall outside the scope of liability, but once a plaintiff alleges and shows that an intrusion onto their land or body has occurred, that alone creates a concrete and particularized injury that can easily support standing.

---

21 Id. at 597–98.

22 Warren & Brandeis; Prosser.

23 In re Facebook, at 598 (citing *Eichenberger* and *Reporters Committee*).

24 "Facebook's user profiles would allegedly reveal an individual's likes, dislikes, interests, and habits over a significant amount of time, without affording users a meaningful opportunity to control or prevent the unauthorized exploration of their private lives." Id. at 598.

25 Analogies to private property are more common in the privacy literature (*see,* e.g., Thomas Kadri, Platforms as Blackacres; Erving Goffman, *The Presentation of Self in Everyday Life*). But as the next section will explain, analogies to control over the body might make more sense. The law allows many intentional de minimis physical contacts to take place (at least in public) without consent. In numerous circumstances, liability is either avoided because the contact was not *offensive* contact or because consent is implied-in-law. These can be thought of as similar to intrusions that are not highly offensive.

In re Facebook also demonstrates that an intrusion can occur even if third parties who are trusted by the plaintiffs facilitate the defendant's intrusion. Recall that in order for Facebook to collect web tracking data, the third party websites had to affirmatively add the Facebook "like" button and the accompanying HTML code that copied and routed website retrieval requests to Facebook. Those third-party websites are entitled to access and collect information about the visitors to their website. Indeed, they *have to* have access to this data in order for the website to work. If the third-party websites' collections of data are not intruding on the plaintiffs' seclusion, how can it be that Facebook's collection of the same data, with the permission of those third-party websites, is intrusive?

The court does not answer this directly.[26] But the answer is straightforward. Even if the third-party websites have valid access to the plaintiffs' seclusion, they are not permitted to bring onlookers. Thus, for the same reason that Dr. DeMay's friend was not permitted to observe a live birth under the pretenses of being a medical assistant in the famous 19th century intrusion case,[27] Facebook is not permitted to observe the data that seclusion insiders may have. The third-party websites therefore must also share responsibility, as they facilitated and induced an intrusion by Facebook.

5 The "Highly Offensive" Element Protects the Intruder's Valid Interests

The *In re Facebook* opinion clarifies that Intrusion upon Seclusion has not one but *two* major elements (in addition to the intentional mental state requirement.) "Because of the similarity of the tests, courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive. [] We address both in turn."[28]

To assess whether the intrusion was highly offensive, the court explained that

> [p]laintiffs must show more than an intrusion upon reasonable privacy expectations. Actionable invasions of privacy also must be 'highly offensive' to a reasonable person, and 'sufficiently serious' and unwarranted so as to constitute an 'egregious breach of the social norms.' [] Determining whether a defendant's actions were "highly offensive to a reasonable person" requires a holistic consideration of factors such as the likelihood of serious harm to the victim,

26 The court said that "Facebook facilitated this practice by embedding third-party plug-ins on third-party web pages." In re Facebook at 596. This is actually backwards; the third-parties embedded the plug-ins on their own websites, so it is the third-parties that are facilitating Facebook.

27 DeMay v. Roberts, 9 N.W. 146 (Mich. 1881).

28 Id. at 601.

> the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive. While analysis of a reasonable expectation of privacy primarily focuses on the nature of the intrusion, the highly offensive analysis focuses on the degree to which the intrusion is unacceptable as a matter of public policy.

In other words, the "highly offensive" element asks whether the plaintiffs' loss of control can be justified by the defendant's or society's interests.

This was a revelation for me. I had long thought that the "highly offensive" language functioned to bolster the "seclusion" element – that is, to make sure that the personal information involved in a certain set of facts would only be considered part of the person's "seclusion" if access to it would be highly offensive. Most published opinions do little to distinguish the "highly offensive" from the rest of the analysis concerning whether the plaintiff had a reasonable expectation of privacy. And I am embarrassed to say that for years, I have been teaching the Restatement elements with mocking derision at the fact that all of the elements – seclusion, intrusion, and highly offensive – seem to be asking the same essential question: was the plaintiff justified in expecting nobody would observe her?[29]

In a single paragraph, Judge Thomas elevated the "highly offensive" language to an independent purpose *and* reshaped the Intrusion tort to be a tool for sensible trade-offs. When courts ask how the plaintiff might be harmed by the alleged practices, what the defendant intended to do with the information, and what society gets out of the whole affair, they are recognizing that the legitimate interests of defendants and others are *also* at stake, and the conflict in interests must be managed without giving veto power to anyone.

We can imagine the "seclusion" element capturing the scope of the plaintiff's privacy interests, where the interests are so strong as to be determinative in some contexts and places, but fade gradually in contexts that are less related to the plaintiff's social or physical vulnerabilities. Meanwhile, the idea of non-offensiveness vis-à-vis the plaintiff (the converse of "highly offensive") would define a scope centered around the activities of the defendant and other similarly situated observers. Here, too, there are some contexts where the interests of the observers are so strong as to be determinative, as when a journalist takes a photograph in public. But the interest gradually fades in contexts where the defendant's or the public's interests in observation are less compelling. These two elements and the interaction between them define where the defendant will be liable.

---

29 Even the case that the court quotes, Hernandez v. Hillsdale, 47 Cal.4th 272 (2009), had not previously convinced me that the elements were separate since the public policy considerations, at least in that case, tended to bleed into the analysis of whether the plaintiffs' assertions of privacy rights were reasonable.

6 In re Facebook Asks the Right Questions, but Privacy Advocates Might not Like the Answers

The court did not decide whether Facebook's intrusions were highly offensive. They left that fact-intensive exercise to be determined at the trial that would, of course, never actually occur.[30] Which party would have had the better argument with respect to the "highly offensive" element?

Let's revisit the factors:

> Determining whether a defendant's actions were "highly offensive to a reasonable person" requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive.

Likelihood of serious harm-this part of the "highly offensive" analysis allows courts to peek at the *use* of personal information in order to determine whether its acquisition was legal. A business that accesses geolocation data in order to create more effective advertising will be viewed with less suspicion than a jealous ex-boyfriend who accesses the same data. While opinions about behavioral marketing are varied, few would say that they cause *serious* harm. Indeed, some of the "victims" may positively benefit from Facebook's practices. While the victim's interests in privacy are misaligned with Facebook's interests, the victim's interests in continuing to receive $0 price high quality social media services are dependent on Facebook having a viable strategy to bring in revenues and sustain its existence.[31]

---

30 The case was settled on _ date_.

31 Empirical research shows that websites would lose between 38 and 66 % of their advertising revenues if behavioral advertising is banned. Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57 MGMT. SCI. 57 (2011) (65 % reduction in revenue); Howard Beales & Jeffrey A. Eisenach, *An Empirical Analysis of the Value of Information Sharing in the Market for Online Content* (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2421405 (66 % reduction); Garrett A. Johnson et al., *Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?*, 39 MARKETING SCI. 33 (52 % reduction); Deepak Ravichandran & Nitish Korula, *Effect of Disabling Third-Party Cookies on Publisher Revenue* Google (2019), (64 % reduction); Facebook, The Value of Personalized Ads to a Thriving App Ecosystem (2020) (50 % reduction); Koen Pauwels, What's a Cookie Worth Anyway?, Smarter Marketing Gets Better Results (2021), https://analyticdashboards.wordpress.com/2021/06/28/whats-a-cookie-worthanyway/. The only study that found a lower figure was based on a single high value publisher and assumed that advertisers would still have access to a user's geolocation and device information. Veronica Marotta et al., *Online Tracking and Publishers' Revenues: An Empirical Analysis* (2019), https://weis2019.econinfosec.org/wpcontent/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf. Ad-blocking may also diminish the quantity and quality of ad-supported websites. Benjamin Shiller et al., The Effect of Ad Blocking on Website Traffic and Quality, 49 RAND J. ECON. 43 (2018) (showing that ad-blocking software, which decreases the effectiveness of

The degree and setting of the intrusion- This factor seems to harken back to the seclusion analysis. In scenarios where there is a degree of seclusion and also a degree of legitimacy for the observer's activity, the scale of invasiveness of the intrusion should affect the court's determination of the tort. If the interests in seclusion are great and the countervailing interests of the observer are weak, the observation is more offensive. Reasonable minds will disagree on whether Facebook should win or lose this factor. On one hand, Facebook's privacy policy provided false assurances that they would not track users who were logged out of their Facebook profiles, and this deceit may have given users false confidence that their web visits were not being tracked and strung together. What's more, the cross-website tracking involves the observation of users who are often in physically private spaces such as their homes. On the other hand, the typical Facebook user probably tolerates tracking of their web browsing behavior by several other cookies, browsers, and other technologies, suggesting that surfing from site to site is more "public" than "private"– more like transiting through physical space between buildings.

The intruder's motives and objectives- Facebook's motives are to improve their advertising business by better matching advertisers and Facebook users and thereby commanding higher ad prices.[32] The websites facilitating Facebook's intrusions have their own objectives – namely, to collect information and have their own Facebook presence promoted in Facebook's algorithms. None of the intruders have a desire or specific intent to cause harm to the plaintiffs unless effective advertising is treated as a sort of attack on the willpower or independence of the Facebook user. Instead, Facebook and the websites that work with it are interested in bolstering their place in the digital economy. Facebook is also interested in generating enough revenue to more than cover the costs of providing a free social networking service.

Countervailing interests and norms: Finally, there may be other norms or public and private interests that run in favor of the freedom to observe. In this case, most of the interests and norms may already be accounted for in the factors that have already been discussed. A more general way to pull together the interests involved in this case, though, is as follows: the commercial Internet that most users have grown

---

advertising in ways that would have a similar revenue impact to a ban on targeted advertising, caused the quality of ad-supported websites to decrease); Garrett Johnson, The Impact of Privacy Policy on the Auction Market for Online Display Advertising (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2333193. *But see* V. Lefrere et al., *The Impact of GDPR on Content Providers: A Longitudinal Analysis,* NBER Working Paper (2022) (finding no significant reduction in the amount of content produced by EU-based websites as compared to US-based websites).

32 Ads placed without behavioral advertising have much smaller click-through rates, and thus generate much less revenue for Facebook as an ad placer. *See.* Garrett A. Johnson et al., *Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry?*, 39 Marketing Sci. 33 (finding ads placed for profiles that opted out of tracking command a 50 % lower price).

accustomed to, with varying degrees of awareness and acquiescence, is one in which services are routinely underwritten by the proceeds from highly targeted advertising. Disrupting these norms and business models for the sake of user privacy may be justified, but there is little doubt that there *are* norms and expectations that will be upset and altered.

Given that Facebook, the third party websites, and, indirectly, the Facebook users benefit from the behavioral advertising-based free Facebook services, it is far from clear that Facebook's data collection was highly offensive. Indeed, in the future, courts may even come to demand that the plaintiff allege more specific facts that substantiate the claim that the defendant's intrusion was highly offensive in order to survive a summary judgment motion. This would bring the Intrusion tort into better alignment with public policy principles that regard information-gathering as a socially beneficial activity.

7 Conclusions

In re Facebook offers an important exploration into the modern dynamics of the Intrusion Upon Seclusion tort, and perhaps the other privacy torts as well. In particular, the distinction between the seclusion element (the plaintiff's reasonable expectation of privacy) and the "highly offensive" element is crucial. The division of labor between these elements allows for a sophisticated balancing between the privacy interests, which may be determinatively strong in some contexts and present-but-weak in others, and the information-gathering interests of others and the practical realities of modern, technologically-infused life.

The factors presented for determining the offensiveness of an intrusion are comprehensive, but their application is bound to be contentious. As privacy concerns continue to evolve with technological innovation, this case serves as a testament to the need for the legal framework to be adaptable.