

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JUSTIN GRAHAM, on behalf of himself and
all others similarly situated,

Plaintiff,

v.

BLOOMBERG L.P.,

Defendant

Civil Action No.

JURY TRIAL DEMANDED

CLASS ACTION

CLASS ACTION COMPLAINT

INTRODUCTION

Plaintiff Justin Graham, on behalf of himself and all others similarly situated, files this Complaint against Defendant Bloomberg L.P. (“Bloomberg” or “Defendant”) for violation of the federal Video Privacy Protection Act, 18 U.S.C. § 2710 (“VPPA”). Plaintiff’s claims arise from Defendant’s practice of knowingly disclosing to a third party, Meta Platforms, Inc. (“Facebook”), data containing its digital subscribers’ (i) personally identifiable information or Facebook ID (“FID”) and (ii) the computer file containing video and its corresponding URL viewed (“Video Media”) (collectively, “Personal Viewing Information”). Plaintiff’s allegations are made on personal knowledge as to Plaintiff and Plaintiff’s own acts and upon information and belief as to all other matters.

I. NATURE OF THE ACTION

1. This is a consumer digital privacy class action complaint against Bloomberg, as the owner of *Bloomberg.com*, for violating the VPPA by disclosing its digital subscribers’ identities and Video Media to Facebook without the proper consent.

2. The VPPA prohibits “video tape service providers,” such as *Bloomberg.com*, from knowingly disclosing consumers’ personally identifiable information, including “information which identifies a person as having requested or obtained specific video materials or services from a video tape provider,” without express consent in a stand-alone consent form.

3. Like other businesses with an online presence, Defendant collects and shares the personal information of visitors to its website and mobile application (“App”) with third parties. Defendant does this through cookies, software development kits (“SDK”), and pixels. In other words, digital subscribers to *Bloomberg.com* have their personal information disclosed to Defendant’s third-party business partners.

4. The Facebook pixel is a code Defendant installed on the *Bloomberg.com* website allowing it to collect users’ data. More specifically, it tracks when digital subscribers enter the *Bloomberg.com* website or App and view Video Media. The *Bloomberg.com* website tracks and discloses to Facebook the digital subscribers’ viewed Video Media, and most notably, the digital subscribers’ FID. This occurs even when the digital subscriber has not shared (nor consented to share) such information.

5. Importantly, Bloomberg shares the Personal Viewing Information—i.e., digital subscribers’ unique FID and video content viewed—*together as one data point to Facebook*. Because the digital subscriber’s FID uniquely identifies an individual’s Facebook user account, Facebook—or any other ordinary person—can use it to quickly and easily locate, access, and view digital subscribers’ corresponding Facebook profile. Put simply, the pixel allows Facebook to know what Video Media one of its subscribers viewed on the *Bloomberg.com* site.

6. Thus, without telling its digital subscribers, Defendant profits handsomely from its unauthorized disclosure of its digital subscribers' Personal Viewing Information to Facebook. It does so at the expense of its digital subscribers' privacy and their statutory rights under the VPPA.

7. Because *Bloomberg.com* digital subscribers are not informed about this dissemination of their Personal Viewing Information – indeed, it is automatic and *invisible* – they cannot exercise reasonable judgment to defend themselves against the highly personal ways *Bloomberg.com* has used and continues to use data it has about them to make money for itself.

8. Defendant chose to disregard Plaintiff's and hundreds of thousands of other *Bloomberg.com* digital subscribers' statutorily protected privacy rights by releasing their sensitive data to Facebook. Accordingly, Plaintiff brings this class action for legal and equitable remedies to redress and put a stop to Defendant's practices of intentionally disclosing its digital subscribers' Personal Viewing Information to Facebook in knowing violation of VPPA.

II. JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over the claims that arise under the Video Privacy Protection Act, 18 U.S.C. § 2710.

10. This Court also has jurisdiction under 28 U.S.C. § 1332(d) because this action is a class action in which the aggregate amount in controversy for the proposed Class (defined below) exceeds \$5,000,000, and at least one member of the Class is a citizen of a state different from that of Defendant.

11. Venue is appropriate in this District pursuant to 28 U.S.C. §1391 because Defendant does business in and is subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claim occurred in or emanated from this District.

III. THE PARTIES

12. Plaintiff Justin Graham is a natural person and resident and citizen of the State of Florida residing in the City of Orlando. Plaintiff began his paid digital subscription to *Bloomberg.com* in approximately February of 2021 and maintained his subscription until approximately May 2021. Plaintiff has had a Facebook account from approximately July 2009 to the present. During the relevant time period, he has used his *Bloomberg.com* digital subscription to view Video Media through *Bloomberg.com* website and/or App while logged into his Facebook account. By doing so, Plaintiff's Personal Viewing Information was disclosed to Facebook pursuant to the systematic process described herein. Plaintiff never gave Defendant express written consent to disclose his Personal Viewing Information.

13. Defendant, Bloomberg, is a privately held financial, software, data, and media company headquartered in Midtown Manhattan, New York City. Defendant has an estimated annual revenue of approximately \$10 billion. Defendant owns and operates the media website *Bloomberg.com*, which provides a broad selection of video content. As detailed below, through *Bloomberg.com* website and App, Defendant delivers and, indeed, is in the business of delivering, countless hours of video content to its digital subscribers.

IV. FACTUAL ALLEGATIONS

A. Background of the Video Privacy Protection Act

14. The VPPA generally prohibits the knowing disclosure of a customer's video rental or sale records without the informed, written consent of the customer in a form "distinct and separate from any form setting forth other legal or financial obligations." Under the statute, the Court may award actual damages (but not less than liquidated damages of \$2,500.00 per person), punitive damages, equitable relief and attorney's fees.

15. The VPPA was initially passed in 1988 for the explicit purpose of protecting the privacy of individuals' and their families' video rental, purchase and viewing data. Leading up to its enactment, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." S. Rep. No. 100-599 at 7-8 (1988).

16. Senators at the time were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and other audiovisual materials. As Senator Patrick Leahy and the late Senator Paul Simon recognized, records of this nature offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

17. In proposing the Video and Library Privacy Protection Act (later codified as the VPPA), Senator Leahy stated that "[i]n practical terms our right to privacy protects the choice of movies that we watch with our family in our own homes. And it protects the selection of books that we choose to read." 134 Cong. Rec. S5399 (May 10, 1988). Thus, the personal nature of such information, and the need to protect it from disclosure, is the inspiration of the statute: "[t]hese activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id.*

18. While these statements rang true in 1988 when the VPPA was passed, the importance of legislation like the VPPA in the modern era of data mining from online activities is more pronounced than ever before. During a recent Senate Judiciary Committee meeting, "The

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.