

The Everalbum, Inc. Case, or How the Federal Trade Commission Protected Consumer Rights Regarding the Collection, Use, Storage, Dissemination, and Destruction of Facial Recognition Data



Donald L. Buresh, Ph.D., J.D., LL.M.

Morgan State University

ABSTRACT: This essay aims to analyze and evaluate the *In the Matter of Everalbum, Inc.* case. The paper discusses the Ever facial recognition application, its history, how it was developed, and the effects of the user deactivation process. The following section outlines Section 5 of the Federal Trade Commission Act, focusing on unfair trade practices. The third section lists the issues in the case. The fourth section outlines the Decision and Order from the Federal Trade Commission regarding how the Commission demanded how Everalbum was to behave in the future. The comments by David Valentine and World Privacy Forum are summarized. A critique of the Order is provided, noting that by demanding that Everalbum delete and destroy its facial recognition technology, the question of who then owned the technology is paramount. The essay concludes by observing that a balance must be struck between the benefits of employing facial recognition technology and its unknown and possibly unknowable detrimental effects.

KEYWORDS: Everalbum, Inc., Facial Recognition, Controlling Facial Recognition App, Deleting Facial Recognition Data, Deactivation of a Facial Recognition Account, Section 5(a) of the Federal Trade Commission Act

INTRODUCTION

Have you ever seen old photographs that were taken years ago? Did you ever wonder who those people were? Do you know their names or what their lives were like? Probably not. If there was ever a reason for the Ever facial recognition application to exist, the reason was likely to help people remember who they were by identifying their ancestors and friends. As time goes by, people may forget the influential people in their lives years ago, mainly when they were children and when family friend relationships were given but presently not remembered.

Everalbum, Inc. (Everalbum) probably developed their facial recognition technology to help their customers remember, identify, and catalog the images of their friends and family of years past. To do so required developing a new technology, facial recognition technology, that could aid in this identification and cataloging process. However, like any technology, it can benefit its users, but it can also be employed in untold detrimental ways. In analyzing *In the Matter of Everalbum, Inc.*, it should be remembered Everalbum did not likely possess the malicious intent to violate their users' rights of privacy. The facial recognition technology was developed to help people remember their past, for without knowledge of the past and where one comes from, a person will not necessarily know why they are where they are, nor will they understand where they are going. To this end, the Everalbum case bears particular relevance in appreciating the evolution of privacy rights in the United States.

EVERALBUM'S FACIAL RECOGNITION APPLICATION

This section consists of three subsections. The first subsection discusses the Ever facial recognition feature. The second subsection talks about how Everalbum employed user photos and videos to train the firm's facial recognition software to identify individuals. The final subsection examines Everalbum's deactivation process and what occurred and did not occur when a user deactivated their account.

THE EVER FACIAL RECOGNITION FEATURE

Everalbum is a Delaware corporation whose principal place of business is in San Francisco, California.¹ The company sold Ever, photo storage, and organization application, to consumers on iOS and Android operating systems. Across the planet, there were

¹ *In the Matter of Everalbum, Inc.*, UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE COMMISSION (May 7, 2021), available at https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_complaint_final.pdf,

The Everalbum, Inc. Case, or How the Federal Trade Commission Protected Consumer Rights Regarding the Collection, Use, Storage, Dissemination, and Destruction of Facial Recognition Data

approximately 12 million consumers that employ Ever.² The app permitted consumers to upload photos and videos to the Everalbum cloud servers from an individual's mobile device, computer, social media accounts such as Facebook or Instagram, or cloud-based storage facilities such as Dropbox or One Drive.³ The software employed various automated features to help users organize their photos and videos into albums based on where they were taken and the date and time associated with the photo or video.

In February 2017, Everalbum began offering its "Friends" feature that employed facial recognition software to organize the faces of an individual's friends into an electronic album.⁴ A user could identify a photo by tags such as a name or an alias. By default, the application was provided to all Ever users, where a user could not turn off or disable the feature. Beginning in May 2018, Everalbum provided users that were located in Illinois, Texas, and Washington or the European Union (EU) with a pop-up message, asking whether an individual would allow Ever to use facial recognition software. Users who resided in Illinois, Texas, and Washington, or the EU, were given this option because these three states and the EU had passed biometric privacy laws.⁵ In particular, the Illinois law, entitled the *Biometric Information Privacy Act*, is the most stringent and comprehensive of the biometric privacy laws of the three states because it permits private action, whereas only the Attorneys General of Texas or Washington may sue a defendant for a violation of their privacy law.⁶ As for the EU, in June 2018, the General Data Protection Regulation became effective.⁷ Thus, it was reasonable for Everalbum to provide this facility to users living in these three states. It should be pointed out that the privacy acts of California, Nevada, Maine, Virginia, and Colorado did not become law until several years later.⁸

The default value of the Friends feature of Ever was off for these three states. A user was asked to select the Yes button that was displayed in a dialog box. Users located in Illinois, Texas, Washington, or the EU could turn the facial recognition feature on or off.⁹ Beginning in July 2018, Everalbum posted an article on its Help web page describing facial recognition. One statement said that "[w]hen face recognition is turned on, you letting us know that it's ok for us to use face embeddings of the people in your photos and videos, including you, and that you have the approval of everyone featured in your photos and videos."¹⁰ The problem with this statement was that users living outside of Illinois, Texas, and Washington, or the EU could not turn the facial recognition software on or off because it was on by default.¹¹ The article misled users not residing in Illinois, Texas, or Washington, or the EU. In April 2019, Everalbum allowed users not living in Illinois, Texas, Washington, or the EU to have the same features as individuals residing in these three states. In other words, as of April 2019, all users, no matter where they live, could turn facial recognition on or off.¹² According to the FTC complaint, when Ever users were given the option to turn facial recognition on or off, 25 percent or 75,000 of about 300,000 chose to turn the facial recognition application off.¹³

PHOTOS AND VIDEOS THAT TRAINED THE FIRM'S FACIAL RECOGNITION SOFTWARE

In February 2017, when Everalbum began using face recognition, the company employed publicly available facial recognition technology. However, shortly after that, the firm started developing its facial recognition application.¹⁴ To test Ever's facial recognition algorithm, the organization employed the photos from Ever users with or without their consent. From September 2017 to August 2019, Everalbum collected millions of facial images from both its facial recognition database and from data sets that were publicly available to generate four face recognition data sets used in developing the firm's facial recognition software. In April 2018, Everalbum generated its second data set but did not use any facial images of people that thought to be living in the United States or the EU. After testing the facial recognition application that the company had developed in Fall 2017 and April 2018, the firm abandoned the facial recognition technology that it had initially created. In June 2018, Everalbum generated a third data set that excluded users that the company believed were residing in Illinois, Texas, or Washington, or the EU based on the user's IP

² Id.

³ Id.

⁴ Id.

⁵ Donald L. Buresh, *Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, 38 SANTA CLARA UNIVERSITY: HIGH TECH LAW JOURNAL, (Expected publication date: October 2021).

⁶ Id.

⁷ Id.

⁸ Id. Here the California Consumer Privacy Act was effective on June 28, 2018 and was amended by the California Privacy Rights Act in November 2020; the Nevada privacy law went into force on May 29, 2019; the Maine privacy law went into effect on July 1, 2020; Virginia's Consumer Data Protection Act was signed into law on March 2, 2021; and Colorado's Privacy Act officially became law on July 8, 2021.

⁹ *In the Matter of Everalbum, Inc.*, *supra*, note 1.

¹⁰ Id.

¹¹ Id.

¹² Id.

¹³ Id.

¹⁴ Id.

The Everalbum, Inc. Case, or How the Federal Trade Commission Protected Consumer Rights Regarding the Collection, Use, Storage, Dissemination, and Destruction of Facial Recognition Data

address.¹⁵ In August 2019, Everalbum created a fourth data set, but this time excluded users that had neither turned on or off the Ever facial recognition technology. Instead, the company used the facial recognition technology that Paravision produced, an enterprise brand of Everalbum that provided facial recognition for security, access control, and facilitating payments.¹⁶ The facial images collected by Ever were not shared with Paravision's customers.

EVERALBUM'S DEACTIVATION PROCESS

As part of the Ever application, Everalbum users could deactivate their Ever accounts. Since January 2017, about 36,000 users have deactivated their accounts.¹⁷ When a user deactivated their account, the application reminded them that they would lose their photos and albums. Ever showed the user how many pictures and albums would be lost. After a user indicated they wanted to deactivate their account, the software asked a user last time if they were sure they wanted to deactivate their account. If a user again answered yes, the account was deactivated.¹⁸

Everalbum's privacy policy stated that even after a user's account has been deactivated, the company could "retain and use [a user's] information for a certain period to comply with [the company's] legal obligations, resolve disputes, and enforce [the firm's] agreements."¹⁹ However, until at least October 2019, Everalbum failed to delete the photos and albums of users that had deactivated their accounts. The deletion process began after October 2019, and the company only deleted those accounts that were deactivated for longer than three months.²⁰

FEDERAL TRADE COMMISSION ACT: UNFAIR TRADE PRACTICES

According to the FTC, Everalbum violated Section 5(a) of the Federal Trade Commission Act, or 15 U.S. Code § 45, which states that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."²¹ The Act authorized the Commission to prevent persons, partnerships, or corporations, except banks, savings and loan institutions, Federal credit unions, common carriers, domestic and foreign air carriers, and entities subject to the Packers and Stockyards Act of 1921 as amended, from engaging in unfair competitive methods or being involved in unfair or deceptive acts or practices that concern commerce.²² Except under specific circumstances, as stated in the Act, the FTC Act does not apply to unfair methods of competition that deal with trade with foreign nations.²³ According to the Act, unfair or deceptive acts or practices encompass acts or practices that will probably cause foreseeable harm or involves material harm within the United States.²⁴ The remedies that the Commission may impose in the presence of unfair or deceptive acts are described within the Act.

ISSUES ADDRESSED IN THE MATTER OF EVERALBUM, INC.

In the FTC case against Everalbum, two counts were listed. The first count involved a misrepresentation about whether an Ever user could control the application's facial recognition feature.²⁵ By default, Everalbum employed facial recognition for all Ever users who resided anywhere outside Illinois, Texas, Washington, or the EU. The company did not give these users the ability to turn the facial recognition application on or off. Thus, the statements contained in the Help section of its website (everalbum.com) were either false or misleading.

The second count was concerned with misrepresentations regarding deleting users' photos and albums when their accounts were deactivated.²⁶ Everalbum told its users, either directly or indirectly, expressly or implicitly, that Everalbum would delete a user's photos and albums once they deactivated their account. Instead, Everalbum never deleted a user's photos and albums. Thus, Everalbum's Privacy Policy, where the company said that they "[they would] try to delete [user] information as soon as possible upon request," was false or misleading.²⁷

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *Id.*

²¹ See 15 U.S. Code § 45 (a)(1), LEGAL INFORMATION INSTITUTE, available at <https://www.law.cornell.edu/uscode/text/15/45>.

²² See 15 U.S. Code § 45 (a)(2), LEGAL INFORMATION INSTITUTE, available at <https://www.law.cornell.edu/uscode/text/15/45>.

²³ See 15 U.S. Code § 45 (a)(3), LEGAL INFORMATION INSTITUTE, available at <https://www.law.cornell.edu/uscode/text/15/45>.

²⁴ See 15 U.S. Code § 45 (a)(4), LEGAL INFORMATION INSTITUTE, available at <https://www.law.cornell.edu/uscode/text/15/45>.

²⁵ *In the Matter of Everalbum, Inc.*, *supra*, note 1.

²⁶ *Id.*

²⁷ *Id.*

The Everalbum, Inc. Case, or How the Federal Trade Commission Protected Consumer Rights Regarding the Collection, Use, Storage, Dissemination, and Destruction of Facial Recognition Data

DECISION AND ORDER OF THE FEDERAL TRADE COMMISSION

The Decision and Order that the FTC handed down contained eight provisions.²⁸ In the first provision, Everalbum and its officers, agents, employees, and anyone who received actual notice of the Order, were required by the FTC not to misrepresent how it collects, uses, discloses, maintains, or deletes covered information.²⁹ The first provision also demanded that the company limit access to covered information. The duration of time that Everalbum continued to retain customer information after a user deactivated their account was addressed in the provision. Finally, the first provision stated that Everalbum was required to protect the “privacy, security, availability, confidentiality, or integrity of any [c]overed [i]nformation.”³⁰

The second provision required Everalbum and its subsidiaries to clearly and conspicuously reveal its privacy policy, terms of use, and the purposes for which the entity collected and shared a user’s biometric information. This provision required the firm to obtain a user’s consent regarding the collection of their biometric information. Finally, the FTC limited Everalbum’s compliance only to products and services that were offered to users within the United States.³¹ The third provision stipulated that within 30 days of the Order being issued, Everalbum was required to delete all photos and videos from users that asked that their Ever accounts be deactivated. Everalbum had to give the Commission a sworn written statement that the information was deleted or destroyed.³² The third provision also required that within 90 days after the FTC Order had been issued, Everalbum must delete or destroy all face embeddings based on collected biometric information and all affected work product. Again, Everalbum had to furnish the Commission with a sworn written statement confirming that the deletion or destruction was accomplished.³³

The fourth provision insisted that Everalbum acknowledge the receipt of the FTC Order within ten days of the Order being issued. This provision also required that the firm distribute a copy of the Order to all individuals or organizations currently affiliated with Everalbum or associated with Everalbum in the future. The Order had to be delivered ten days after the Order’s effective date to individuals presently associated with Everalbum and for future affiliates before they begin work.³⁴ All persons that received a copy of the Order were required to sign an acknowledgment form, indicating that they had received a copy of the Order.

The fifth provision demanded that Everalbum send the Commission a sworn written compliance report one year after the Order was issued. The report would describe in detail how the firm was complying with the Order. In this provision, the Commission also obliged Everalbum to submit another compliance report within 14 days of any change in the point of contact, structure, control, ownership interest, plus any merger, sale, bankruptcy, or dissolution of the company.³⁵ The sixth provision dealt with record-keeping, where Everalbum needed to maintain accounting records, personal records, and consumer complaints. The condition also compelled the company to generate a document describing how Everalbum protected the privacy, security, availability, confidentiality, or integrity of any covered information obtained from their website, mobile application, or any other service controlled Everalbum.³⁶

The seventh provision expected Everalbum to submit additional compliance reports when requested by the Commission within ten days of receiving a request. The provision authorized the Commission to communicate directly with the company or any person associated with the firm who agreed to be interviewed. The Commission could use any lawful means to achieve a compulsory process.³⁷ The final provision stated that the Order would terminate 20 years from the date that the Order was issued, or 20 years from the most recent date that the United States or the Commission filed a future complaint with or without a future settlement. This final provision put Everalbum under the FTC microscope for many years to come, if not forever.³⁸

COMMENTS REGARDING THE DECISION AND ORDER

This section of the paper is divided into two parts. The first subsection highlights the response by the FTC to the comments made

²⁸ *In the Matter of Everalbum, Inc. Decision and Order*, UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE COMMISSION (May 6, 2021), available at https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf.

²⁹ *Id.* Covered information included (1) first and last name; (2) physical address; (3) email address or any other online address such as an instant messaging address; (4) telephone number; (5) Social Security number; (6) driver’s license or other government identification number; (7) financial account number; (8) debit or credit card number; (9) photos and videos; (10) biometric information as defined in the Decision and Order; (11) descriptive information such as facial embedding; (12) a persistent identifier such as an IP address, mobile device ID, etc.; or (13) any combined information as listed therein.

³⁰ *Id.*

³¹ *Id.*

³² *Id.*

³³ *Id.*

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.*

³⁸ *Id.*

The Everalbum, Inc. Case, or How the Federal Trade Commission Protected Consumer Rights Regarding the Collection, Use, Storage, Dissemination, and Destruction of Facial Recognition Data

by David Valentine. The second subsection outlines the answer by the FTC to the concerns expressed by the World Privacy Forum.

COMMENT TO DAVID VALENTINE

Although the FTC acknowledged that comments made by Valentine generally supported the Decision and Order, Valentine opined that the Order is unfair to consumers outside the United States.³⁹ The FTC believed that consumers both inside and outside the United States were adequately protected regarding notice and consent in the employment by Everalbum of biometric information that the company would use to develop their facial recognition technology. The Commission reminded Valentine that if Everalbum decided to offer a facial recognition application in a foreign country, the firm would be subject to laws and regulations that are significantly more stringent than in the United States.⁴⁰ In particular, it seems that FTC was alluding to the EU General Data Protection Regulation.

COMMENT TO THE WORLD PRIVACY FORUM

In its response to the comments made by the World Privacy Forum (WPF), the Commission addressed the six concerns of the WPF.⁴¹ The FTC acknowledged that the WPF's concerns generally supported the Decision and Order. The government agency attempted to assure the WPF that apprehensions were seriously considered. First, the WPF recommended that the definition of "biometric information" be changed to include "any image from which one can extract an identifying template."⁴² The FTC felt that the current definition of biometric information encompassed any physical or biological traits that could be employed to identify an individual, such as movements or gestures, including gait, typing pattern, sleep, health, or exercise data.⁴³

The second issue expressed by the WPF was that the definition of the term "clearly and conspicuously" included video conferencing. The Commission believed that video conferencing was incorporated into the meaning of the term. The third recommendation by the WPF was that the definition of "face embedding" should contain probabilistic facial embeddings (PFEs), where a facial recognition algorithm outputs a distributional estimation of whether an individual's face was recognized. The FTC opined that the deletion requirements appropriately dealt with facial embeddings.⁴⁴

The fourth concern by the WPF was that the Commission adds language to the Order's notice and consent provision to "state explicitly that it applies to the use of biometric information collected from a user to create 'any type of' face embedding."⁴⁵ The fourth proposal by the WPF was that the definition of face embedding included the employment of biometric information that could be used to utilize, train, develop, or alter any facial recognition algorithm or model. The fifth comment by the WPF asked the FTC to make Everalbum's compliance report freely available to the public instead of requiring the public to file a Freedom of Information Act (FOIA) request.⁴⁶ The Commission rejected this request because it could reveal Everalbum's trade secrets or confidential commercial or financial information.⁴⁷ The final recommendation by the WPF was that the Commission impose a financial penalty on Everalbum. The FTC responded to this proposal by noting that under Section 5 of the Federal Trade Commission Act, civil penalties were not authorized by law for first-time offenders. The FTC suggested that the WPF petition Congress to change the law.⁴⁸

CONSEQUENCES OF THE FTC'S DECISION AND ORDER

This section of this essay is broken up into two subsections. The first subsection addresses the consequences to individuals of the Order, whereas the second subsection is about the effects of the Order on the general public.

CONSEQUENCES OF THE ORDER TO INDIVIDUALS

The FTC's Decision and Order consequences can be readily obtained by evaluating the Order's provisions regarding their effect on individuals. The second provision of the Order directly affects individuals because it demanded that Everalbum disclose its privacy policy, terms of use, and the purposes for which the entity collects and shares a user's biometric information. The second provision

³⁹ *Letter to the Commenter David Valentine*, FEDERAL TRADE COMMISSION (May 6, 2021), available at https://www.ftc.gov/system/files/documents/cases/valentine_response_final.pdf.

⁴⁰ *Id.*

⁴¹ *Letter to the Commenter World Privacy Forum*, FEDERAL TRADE COMMISSION (May 6, 2021), available at https://www.ftc.gov/system/files/documents/cases/wpf_response_final_0.pdf.

⁴² *Id.*

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ *Id.*

The Everalbum, Inc. Case, or How the Federal Trade Commission Protected Consumer Rights Regarding the Collection, Use, Storage, Dissemination, and Destruction of Facial Recognition Data

required Everalbum to obtain a user's consent when their biometric information is collected.⁴⁹ The third provision obliged Everalbum to delete all photos and videos from users that asked that their Ever accounts be deactivated within 30 days of the Order being issued. The third provision of the Order also ensured that the company deleted or destroyed all facial embeddings or work products associated with collecting a user's biometric information.⁵⁰

One consumer issue brought up by Valentine was that the Order was unfair to consumers outside the United States.⁵¹ Although the FTC believed that this was a valid concern, the Commission reminded Valentine that if Everalbum decided to offer facial recognition technology in a foreign country, the firm would probably be subject to the laws of that nation.⁵² In particular, the FTC was likely referring to the EU's General Data Protection Regulation. The result was that the FTC thought that the Order probably addressed the consequences to individuals regarding Everalbum's violation of the Federal Trade Commission Act.

CONSEQUENCES OF THE ORDER ON THE GENERAL PUBLIC

The consequences of the Order on the general public are manifold. The fourth provision of the Order required Everalbum to distribute a copy of the Order to all individuals and organizations affiliated with the firm.⁵³ This action benefited the general public because the public could rest assured that their facial recognition data is secure, private, and confidential. The fifth provision demanded that Everalbum submit a sworn written compliance report to the Commission one year after receiving the Order.⁵⁴ This stipulation further promised the public that their biometric data was secure, private, and confidential. The sixth provision went one step further by obliging Everalbum to maintain accounting, personal, and consumer complaints regarding covered information. The seventh provision required Everalbum to produce compliance reports when demanded by the Commission.⁵⁵ The final condition guaranteed the general public that the FTC would be monitoring the activities of Everalbum for 20 or more years into the future.⁵⁶

The comments by the WPF were of interest to the general public. The WPF wanted the FTC to change the definitions of "biometric information," "clearly and conspicuously," and "facial embedding" to give them greater breadth.⁵⁷ The WPF opined that Everalbum's compliance report should be publicly available, but the FTC appropriately stated that a FOIA request was essential to prevent the disclosure of Everalbum's trade secrets and the company's confidential commercial and financial information.⁵⁸ The decision by the Commission was fair to Everalbum because the FTC is mandated by federal law to protect the company's information appropriately.

CRITIQUE OF THE DECISION AND ORDER

There are several nuances in the Order that deserve to be critiqued. First, according to the Perkins Coie LLP, the Everalbum settlement signaled businesses that FTC is now concentrating on facial recognition technology in particular and biometric data-based technology in general.⁵⁹ It is the first time that the FTC has engaged in an enforcement action regarding facial recognition technology.⁶⁰ The Order imposed strict and broad requirements on Everalbum, demanding that the company delete all facial recognition data collected without a user's consent and destroy all models and algorithms based on the data collected from Ever users. This was a highly disruptive demand because it represented an existential threat to the existence of the business.⁶¹ According to Rattigan, the Ever app has been defunct since August 2020.⁶² Also, this obligation seems to outlaw a mathematical formula. The Order does not address that mathematical formula are true and immutable and can be rediscovered or reverse-engineered by a third party. There was no guarantee that some brilliant mathematician would figure out Everalbum's algorithm and then recreate it. The Order also did not address who owns the trade secrets, copyrights, or patent rights to Everalbum's algorithm. The Order did not

⁴⁹ *In the Matter of Everalbum, Inc. Decision and Order*, *supra*, note 28.

⁵⁰ *Id.*

⁵¹ *Letter to the Commenter David Valentine*, *supra*, note 39.

⁵² *Id.*

⁵³ *In the Matter of Everalbum, Inc. Decision and Order*, *supra*, note 28.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ *Letter to the Commenter World Privacy Forum*, *supra*, note 41.

⁵⁸ *Id.*

⁵⁹ *Everalbum Settles FTC Claims Alleging Deceptive Use of Facial Recognition Technology*, PERKINS COIE (Jan. 29, 2021), available at <https://www.perkinscoie.com/en/news-insights/everalbum-settles-ftc-claims-alleging-deceptive-use-of-facial-recognition-technology.html>.

⁶⁰ *Id.*

⁶¹ *Id.*

⁶² Kathryn M. Rattigan, *Everalbum Settles with FTC over Facial Recognition Technology in its Ever App*, THE NATIONAL LAW REVIEW (Jan. 13, 2021), available at <https://www.natlawreview.com/article/everalbum-settles-ftc-over-facial-recognition-technology-its-ever-app>.

The Everalbum, Inc. Case, or How the Federal Trade Commission Protected Consumer Rights Regarding the Collection, Use, Storage, Dissemination, and Destruction of Facial Recognition Data

answer whether Everalbum is abandoning its trade secrets, copyrights, or patent rights when complying with the FTC to delete or destroy the algorithm. Suppose the Order implied that Everalbum's trade secrets, copyrights, or patent rights had been abandoned. In that case, a question naturally arises as to whether a third party could legally copyright or patent the algorithm or own the algorithm as a trade secret. Of course, Everalbum would argue that the trade secrets, copyrights, or patent rights belong to the company. A third party could effectively say that the deletion and destruction of the algorithm essentially voided those rights, and thus those rights belonged to the third party.

Perkins Coie also observed that the FTC employed its deception authority against a company when Everalbum had no apparent intent to deceive the public.⁶³ The problem with the case was that there was seemingly no requisite consumer injury. The issue for the FTC was that it found Everalbum's behavior problematic at worst.⁶⁴ According to Perkins Coie, the Everalbum Decision and Order would probably result in additional scrutiny of facial recognition technology and other biometric data technologies employed by private businesses.⁶⁵ Although many states have laws like Section 5 of the FTC Act, state regulators may be encouraged to regulate the employment of biometric data strictly. However, currently, only Illinois, Texas, and Washington have passed biometric legislation.^{66 67} As of this writing, California, Nevada, Maine, Virginia, and Colorado are the five states that have passed comprehensive privacy legislation, even though several other states are considering passing biometric data laws.^{68 69} For example, Portland, Oregon, became the first municipality to ban facial recognition technology except under specific circumstances.⁷⁰ It should be noted that Illinois is the only state that possesses a biometric privacy law where private action is permitted.⁷¹ In Texas and Washington, the Attorney General is solely responsible for initiating legal action against a private entity.⁷² Perkins Coie opined that the Everalbum settlement might increase a firm's exposure to private lawsuits such as class actions.⁷³ However, since Illinois is currently the only state that permits private action, this possibility may be overblown.⁷⁴

According to Rattigan, the Everalbum raised more questions than provided answers.⁷⁵ Although the case underscored the possibility of additional consumer class action suits, consumers will probably become more knowledgeable about how facial recognition applications work and are applied in everyday life.⁷⁶ Another issue associated with the settlement was that facial recognition technology might yield more false positives because there was less data to train the artificial intelligence (AI) technology. This fact may adversely affect consumers in ways that are yet unknown to the general public.

CONCLUSION

Given that Everalbum possessed good intentions to help their customers remember their past by cataloging the photos and videos of a time gone by, the case can be considered from various angles. One can take a positive perspective and focus only on the benefits of employing facial recognition technology to help people recall their history. On the other hand, one can recoil in fear that once facial recognition technology has been developed, one loses control of how it will be employed. Both sides of the scale are valid reasons for developing or restricting the technology, respectively. The question becomes which side of the scale is favored. Should society embrace the benefits so that the memory of people who lived years ago may be cherished? Or, should society err on the side of caution and limit the uses of facial recognition technology because of the anxiety that unscrupulous people could use the technology for nefarious purposes? These questions are not easy to answer. If anything has been learned from the Everalbum case, it is that a balance must be struck between the two extremes, where society enjoys the benefits of the technology without experiencing its inevitable, possibly harmful consequences.

In conclusion, the Everalbum case implied that facial recognition applications must be judiciously regulated to ensure that government and corporate needs are satisfied while ensuring that individual privacy is respected. Buresh argued that there is a need in the United States for comprehensive privacy law.⁷⁷ The Everalbum case further emphasized that the need for comprehensive federal privacy legislation demands the attention of Congress. Nothing short of that will suffice.

⁶³ *Everalbum Settles FTC Claims Alleging Deceptive Use of Facial Recognition Technology*, *supra*, note 59.

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ *Id.*

⁶⁷ Donald L. Buresh, *supra*, note 5.

⁶⁸ *Id.*

⁶⁹ *Everalbum Settles FTC Claims Alleging Deceptive Use of Facial Recognition Technology*, *supra*, note 59.

⁷⁰ *Id.*

⁷¹ Donald L. Buresh, *supra*, note 5.

⁷² *Id.*

⁷³ *Everalbum Settles FTC Claims Alleging Deceptive Use of Facial Recognition Technology*, *supra*, note 59.

⁷⁴ Donald L. Buresh, *supra*, note 5.

⁷⁵ Kathryn M. Rattigan, *supra*, note 62.

⁷⁶ *Id.*

⁷⁷ Donald L. Buresh, *supra*, note 5.

The Everalbum, Inc. Case, or How the Federal Trade Commission Protected Consumer Rights Regarding the Collection, Use, Storage, Dissemination, and Destruction of Facial Recognition Data

REFERENCES

1. *In the Matter of Everalbum, Inc.*, UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE COMMISSION (May 7, 2021), available at https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_complaint_final.pdf.
2. Donald L. Buresh, *Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, 38 SANTA CLARA UNIVERSITY: HIGH TECH LAW JOURNAL, (Expected publication date: October 2021).
3. Here the California Consumer Privacy Act was effective on June 28, 2018 and was amended by the California Privacy Rights Act in November 2020; the Nevada privacy law went into force on May 29, 2019; the Maine privacy law went into effect on July 1, 2020; Virginia's Consumer Data Protection Act was signed into law on March 2, 2021; and Colorado's Privacy Act officially became law on July 8, 2021.
4. *In the Matter of Everalbum, Inc.*, *supra*, note 1.
5. See 15 U.S. Code § 45 (a)(1), LEGAL INFORMATION INSTITUTE, available at <https://www.law.cornell.edu/uscode/text/15/45>.
6. See 15 U.S. Code § 45 (a)(2), LEGAL INFORMATION INSTITUTE, available at <https://www.law.cornell.edu/uscode/text/15/45>.
7. See 15 U.S. Code § 45 (a)(3), LEGAL INFORMATION INSTITUTE, available at <https://www.law.cornell.edu/uscode/text/15/45>.
8. See 15 U.S. Code § 45 (a)(4), LEGAL INFORMATION INSTITUTE, available at <https://www.law.cornell.edu/uscode/text/15/45>.
9. *In the Matter of Everalbum, Inc.*, *supra*, note 1.
10. *In the Matter of Everalbum, Inc. Decision and Order*, UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE COMMISSION (May 6, 2021), available at https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf.
11. Covered information included (1) first and last name; (2) physical address; (3) email address or any other online address such as an instant messaging address; (4) telephone number; (5) Social Security number; (6) driver's license or other government identification number; (7) financial account number; (8) debit or credit card number; (9) photos and videos; (10) biometric information as defined in the Decision and Order; (11) descriptive information such as facial embedding; (12) a persistent identifier such as an IP address, mobile device ID, etc.; or (13) any combined information as listed therein.
12. *Letter to the Commenter David Valentine*, FEDERAL TRADE COMMISSION (May 6, 2021), available at https://www.ftc.gov/system/files/documents/cases/valentine_response_final.pdf.
13. *Letter to the Commenter World Privacy Forum*, FEDERAL TRADE COMMISSION (May 6, 2021), available at https://www.ftc.gov/system/files/documents/cases/wpf_response_final_0.pdf.
14. *In the Matter of Everalbum, Inc. Decision and Order*, *supra*, note 28.
15. *Letter to the Commenter David Valentine*, *supra*, note 39.
16. *In the Matter of Everalbum, Inc. Decision and Order*, *supra*, note 28.
17. *Letter to the Commenter World Privacy Forum*, *supra*, note 41.
18. *Everalbum Settles FTC Claims Alleging Deceptive Use of Facial Recognition Technology*, PERKINS COIE (Jan. 29, 2021), available at <https://www.perkinscoie.com/en/news-insights/everalbum-settles-ftc-claims-alleging-deceptive-use-of-facial-recognition-technology.html>.
19. Kathryn M. Rattigan, *Everalbum Settles with FTC over Facial Recognition Technology in its Ever App*, THE NATIONAL LAW REVIEW (Jan. 13, 2021), available at <https://www.natlawreview.com/article/everalbum-settles-ftc-over-facial-recognition-technology-its-ever-app>.
20. *Everalbum Settles FTC Claims Alleging Deceptive Use of Facial Recognition Technology*, *supra*, note 59.
21. Donald L. Buresh, *supra*, note 5.
22. *Everalbum Settles FTC Claims Alleging Deceptive Use of Facial Recognition Technology*, *supra*, note 59.
23. Donald L. Buresh, *supra*, note 5.
24. *Everalbum Settles FTC Claims Alleging Deceptive Use of Facial Recognition Technology*, *supra*, note 59.
25. Donald L. Buresh, *supra*, note 5.
26. Kathryn M. Rattigan, *supra*, note 62.
27. Donald L. Buresh, *supra*, note 5.