

January 29, 2020






Kate Romanovskaia, Director, Brand & Communications  
Flo Health Inc.  
1013 Centre Road, Suite 403-B  
Wilmington, DE 19805

Via email to: k\_romanovskaia@flo.health

To whom it may concern:

We the undersigned organizations reach out to urge you to take the lead in improving the privacy standard for health apps such as your own. Reproductive health apps are offered as an empowerment tool for consumers eager for power and agency over their health. Yet at the same time, many health apps do not have proper privacy standards in place, which can result in sensitive health data falling into the wrong hands. The vast majority of Americans report feeling as if they have little or no control over the data collected on them.<sup>i</sup> Users of reproductive health apps have reason to be wary.

There are very few legal privacy restrictions on app developers. That a company has free rein to collect, use, and share user data does not mean that they should – they absolutely should not. Fundamentally, consumers do not expect their intimate health details to be shared with research and advertising companies without their explicit and informed permission. Yet Consumer Reports identified privacy issues with each of the reproductive health apps it recently evaluated, as summarized in the excerpt below.<sup>ii</sup>

					
	BabyCenter	Clue	Flo	My Calendar	Ovia
Is the privacy policy easy to understand?	NO	YES	YES	NO	YES & NO
Can you use without sharing your name and email?	YES	NO	YES	NO	NO
Who does the app share your data with?					
Advertisers and marketers	YES	YES	YES	YES	YES
Health researchers, with your permission	NO	YES	YES	NO	YES
Insurers and employers via wellness programs	NO	NO	NO	NO	YES
Does the app use these 2 security precautions?					
Default is to authenticate the user with each use	NO	NO	NO	YES	NO
Works with password managers	YES	YES	YES	NO	YES

The current state of privacy laws in the United States leaves a patchwork of protections for an individual's personal information with more gaps than coverage. Further, health privacy laws that consumers have relied upon for decades to protect sensitive details about themselves do not extend to direct-to-consumer health

technology such as reproductive health apps. The bar is low. But as a purveyor of wellness, you should aim higher. To that end, we write to urge you to:

1. Only use collected data for the purpose of the health app;
2. Limit the data you collect to only information needed to operate the app;
3. Decline to share or sell user information;
4. Safely destroy collected data once it is no longer needed to operate the app;
5. Give consumers clear and concise information about what you do with their data and why.

Respecting your customers' privacy is a basic and achievable goal. A blueprint for doing so is available in the form of the Digital Standard, a set of benchmarks that companies can use to design digital products that are respectful of consumer privacy rights.<sup>iii</sup> Protecting app users' personal data is also a fundamental civil liberty concern. In the hands of unintended parties, consumer data has been used to create psychological profiles of voters for illicit political purposes<sup>iv</sup>; and enabled businesses to create alternative, nonevidence based and potentially discriminatory, credit scores based on consumers' digital footprint.<sup>v</sup>

Reproductive health apps such as yours must act fairly and transparently so consumers can make informed choices, not only in their care but also in the tools they use to manage their health. Over 22,000 consumers who signed a recent Consumer Reports petition agree. While lawmakers in Washington D.C. and in the states grapple with the right approach to legally secure consumer privacy, we turn to you to hold yourself to a higher standard so consumers can trust that the apps they use to care for themselves are not violating their privacy.

Signed,

Consumer Reports  
ACLU of Washington  
Center for Democracy and Technology  
Common Sense Media  
Digital Privacy Alliance  
Electronic Frontier Foundation  
HumanFirst.Tech  
National Partnership for Women & Families  
National Women's Law Center  
Norwegian Consumer Council  
Privacy Rights Clearinghouse

---

<sup>i</sup> Pew Research Survey, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, (November 15, 2019).

<sup>ii</sup> Donna Rosato, "What your period tracker app knows about you," Consumer Reports (January 16, 2020).

<sup>iii</sup> The Digital Standard was launched by Consumer Reports in 2017 in partnership with privacy and security experts. It is available at <https://www.thedigitalstandard.org/>.

<sup>iv</sup> Ahead of the 2016 presidential election, Cambridge Analytica acquired data on Facebook users through an online entertainment quiz, which was only completed by about 270,000 people but revealed data on 50 million individuals. This was a prominent example of how data collected through seemingly innocuous ways can be used for illicit purposes. Jerry Beilinson, "Facebook Data May Have Been Illicitly Used for Politics, and It Started With a Quiz", Consumer Reports (March 17, 2018).

<sup>v</sup> National Bureau of Economic Research, Working Paper: On the Rise of FinTechs – Credit Scoring Using Digital Footprints, (April 2018, Revised July 2018). This study raises the concern that the digital footprint may be used as a proxy for legally prohibited variables – such as race, color, gender, national origin, and religion – which can lead to discrimination.

January 29, 2020

Ryan Duncan, Strategic Communications & PR Manager

BioWink, parent company of Clue

Clue by BioWink






Adalbertstraße 8, D-10999, Berlin

Via email to: ryan@helloc clue.com

To whom it may concern:

We the undersigned organizations reach out to urge you to take the lead in improving the privacy standard for health apps such as your own. Reproductive health apps are offered as an empowerment tool for consumers eager for power and agency over their health. Yet at the same time, many health apps do not have proper privacy standards in place, which can result in sensitive health data falling into the wrong hands. The vast majority of Americans report feeling as if they have little or no control over the data collected on them.<sup>i</sup> Users of reproductive health apps have reason to be wary.

There are very few legal privacy restrictions on app developers. That a company has free rein to collect, use, and share user data does not mean that they should – they absolutely should not. Fundamentally, consumers do not expect their intimate health details to be shared with research and advertising companies without their explicit and informed permission. Yet Consumer Reports identified privacy issues with each of the reproductive health apps it recently evaluated, as summarized in the excerpt below.<sup>ii</sup>

					
	BabyCenter	Clue	Flo	My Calendar	Ovia
<b>Is the privacy policy easy to understand?</b>	NO	YES	YES	NO	YES & NO
<b>Can you use without sharing your name and email?</b>	YES	NO	YES	NO	NO
<b>Who does the app share your data with?</b>					
Advertisers and marketers	YES	YES	YES	YES	YES
Health researchers, with your permission	NO	YES	YES	NO	YES
Insurers and employers via wellness programs	NO	NO	NO	NO	YES
<b>Does the app use these 2 security precautions?</b>					
Default is to authenticate the user with each use	NO	NO	NO	YES	NO
Works with password managers	YES	YES	YES	NO	YES

The current state of privacy laws in the United States leaves a patchwork of protections for an individual's personal information with more gaps than coverage. Further, health privacy laws that consumers have relied upon for decades to protect sensitive details about themselves do not extend to direct-to-consumer health

technology such as reproductive health apps. The bar is low. But as a purveyor of wellness, you should aim higher. To that end, we write to urge you to:

1. Only use collected data for the purpose of the health app;
2. Limit the data you collect to only information needed to operate the app;
3. Decline to share or sell user information;
4. Safely destroy collected data once it is no longer needed to operate the app;
5. Give consumers clear and concise information about what you do with their data and why.

Respecting your customers' privacy is a basic and achievable goal. A blueprint for doing so is available in the form of the Digital Standard, a set of benchmarks that companies can use to design digital products that are respectful of consumer privacy rights.<sup>iii</sup> Protecting app users' personal data is also a fundamental civil liberty concern. In the hands of unintended parties, consumer data has been used to create psychological profiles of voters for illicit political purposes<sup>iv</sup>; and enabled businesses to create alternative, nonevidence based and potentially discriminatory, credit scores based on consumers' digital footprint.<sup>v</sup>

Reproductive health apps such as yours must act fairly and transparently so consumers can make informed choices, not only in their care but also in the tools they use to manage their health. Over 22,000 consumers who signed a recent Consumer Reports petition agree. While lawmakers in Washington D.C. and in the states grapple with the right approach to legally secure consumer privacy, we turn to you to hold yourself to a higher standard so consumers can trust that the apps they use to care for themselves are not violating their privacy.

Signed,

Consumer Reports  
ACLU of Washington  
Center for Democracy and Technology  
Common Sense Media  
Digital Privacy Alliance  
Electronic Frontier Foundation  
HumanFirst.Tech  
National Partnership for Women & Families  
National Women's Law Center  
Norwegian Consumer Council  
Privacy Rights Clearinghouse

---

<sup>i</sup> Pew Research Survey, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, (November 15, 2019).

<sup>ii</sup> Donna Rosato, "What your period tracker app knows about you," Consumer Reports (January 16, 2020).

<sup>iii</sup> The Digital Standard was launched by Consumer Reports in 2017 in partnership with privacy and security experts. It is available at <https://www.thedigitalstandard.org/>.

<sup>iv</sup> Ahead of the 2016 presidential election, Cambridge Analytica acquired data on Facebook users through an online entertainment quiz, which was only completed by about 270,000 people but revealed data on 50 million individuals. This was a prominent example of how data collected through seemingly innocuous ways can be used for illicit purposes. Jerry Beilinson, "Facebook Data May Have Been Illicitly Used for Politics, and It Started With a Quiz", Consumer Reports (March 17, 2018).

<sup>v</sup> National Bureau of Economic Research, Working Paper: On the Rise of FinTechs – Credit Scoring Using Digital Footprints, (April 2018, Revised July 2018). This study raises the concern that the digital footprint may be used as a proxy for legally prohibited variables – such as race, color, gender, national origin, and religion – which can lead to discrimination.

January 29, 2020






Linda Murray, SVP Consumer Experience  
BabyCenter  
163 Freelon Street  
San Francisco, CA 94107

Via email to: linda.murray@babycenter.com

To whom it may concern:

We the undersigned organizations reach out to urge you to take the lead in improving the privacy standard for health apps such as your own. Reproductive health apps are offered as an empowerment tool for consumers eager for power and agency over their health. Yet at the same time, many health apps do not have proper privacy standards in place, which can result in sensitive health data falling into the wrong hands. The vast majority of Americans report feeling as if they have little or no control over the data collected on them.<sup>i</sup> Users of reproductive health apps have reason to be wary.

There are very few legal privacy restrictions on app developers. That a company has free rein to collect, use, and share user data does not mean that they should – they absolutely should not. Fundamentally, consumers do not expect their intimate health details to be shared with research and advertising companies without their explicit and informed permission. Yet Consumer Reports identified privacy issues with each of the reproductive health apps it recently evaluated, as summarized in the excerpt below.<sup>ii</sup>

					
	BabyCenter	Clue	Flo	My Calendar	Ovia
<b>Is the privacy policy easy to understand?</b>	NO	YES	YES	NO	YES & NO
<b>Can you use without sharing your name and email?</b>	YES	NO	YES	NO	NO
<b>Who does the app share your data with?</b>					
Advertisers and marketers	YES	YES	YES	YES	YES
Health researchers, with your permission	NO	YES	YES	NO	YES
Insurers and employers via wellness programs	NO	NO	NO	NO	YES
<b>Does the app use these 2 security precautions?</b>					
Default is to authenticate the user with each use	NO	NO	NO	YES	NO
Works with password managers	YES	YES	YES	NO	YES

The current state of privacy laws in the United States leaves a patchwork of protections for an individual's personal information with more gaps than coverage. Further, health privacy laws that consumers have relied upon for decades to protect sensitive details about themselves do not extend to direct-to-consumer health

technology such as reproductive health apps. The bar is low. But as a purveyor of wellness, you should aim higher. To that end, we write to urge you to:

1. Only use collected data for the purpose of the health app;
2. Limit the data you collect to only information needed to operate the app;
3. Decline to share or sell user information;
4. Safely destroy collected data once it is no longer needed to operate the app;
5. Give consumers clear and concise information about what you do with their data and why.

Respecting your customers' privacy is a basic and achievable goal. A blueprint for doing so is available in the form of the Digital Standard, a set of benchmarks that companies can use to design digital products that are respectful of consumer privacy rights.<sup>iii</sup> Protecting app users' personal data is also a fundamental civil liberty concern. In the hands of unintended parties, consumer data has been used to create psychological profiles of voters for illicit political purposes<sup>iv</sup>; and enabled businesses to create alternative, nonevidence based and potentially discriminatory, credit scores based on consumers' digital footprint.<sup>v</sup>

Reproductive health apps such as yours must act fairly and transparently so consumers can make informed choices, not only in their care but also in the tools they use to manage their health. Over 22,000 consumers who signed a recent Consumer Reports petition agree. While lawmakers in Washington D.C. and in the states grapple with the right approach to legally secure consumer privacy, we turn to you to hold yourself to a higher standard so consumers can trust that the apps they use to care for themselves are not violating their privacy.

Signed,

Consumer Reports  
ACLU of Washington  
Center for Democracy and Technology  
Common Sense Media  
Digital Privacy Alliance  
Electronic Frontier Foundation  
HumanFirst.Tech  
National Partnership for Women & Families  
National Women's Law Center  
Norwegian Consumer Council  
Privacy Rights Clearinghouse

---

<sup>i</sup> Pew Research Survey, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, (November 15, 2019).

<sup>ii</sup> Donna Rosato, "What your period tracker app knows about you," Consumer Reports (January 16, 2020).

<sup>iii</sup> The Digital Standard was launched by Consumer Reports in 2017 in partnership with privacy and security experts. It is available at <https://www.thedigitalstandard.org/>.

<sup>iv</sup> Ahead of the 2016 presidential election, Cambridge Analytica acquired data on Facebook users through an online entertainment quiz, which was only completed by about 270,000 people but revealed data on 50 million individuals. This was a prominent example of how data collected through seemingly innocuous ways can be used for illicit purposes. Jerry Beilinson, "Facebook Data May Have Been Illicitly Used for Politics, and It Started With a Quiz", Consumer Reports (March 17, 2018).

<sup>v</sup> National Bureau of Economic Research, Working Paper: On the Rise of FinTechs – Credit Scoring Using Digital Footprints, (April 2018, Revised July 2018). This study raises the concern that the digital footprint may be used as a proxy for legally prohibited variables – such as race, color, gender, national origin, and religion – which can lead to discrimination.

January 29, 2020

Molly Howard, VP of Operations

Ovia Health

76 Summer Street






Boston, MA 02110

Via email to: molly@oviahealth.com

To whom it may concern:

We the undersigned organizations reach out to urge you to take the lead in improving the privacy standard for health apps such as your own. Reproductive health apps are offered as an empowerment tool for consumers eager for power and agency over their health. Yet at the same time, many health apps do not have proper privacy standards in place, which can result in sensitive health data falling into the wrong hands. The vast majority of Americans report feeling as if they have little or no control over the data collected on them.<sup>i</sup> Users of reproductive health apps have reason to be wary.

There are very few legal privacy restrictions on app developers. That a company has free rein to collect, use, and share user data does not mean that they should – they absolutely should not. Fundamentally, consumers do not expect their intimate health details to be shared with research and advertising companies without their explicit and informed permission. Yet Consumer Reports identified privacy issues with each of the reproductive health apps it recently evaluated, as summarized in the excerpt below.<sup>ii</sup>

					
	BabyCenter	Clue	Flo	My Calendar	Ovia
Is the privacy policy easy to understand?	NO	YES	YES	NO	YES & NO
Can you use without sharing your name and email?	YES	NO	YES	NO	NO
Who does the app share your data with?					
Advertisers and marketers	YES	YES	YES	YES	YES
Health researchers, with your permission	NO	YES	YES	NO	YES
Insurers and employers via wellness programs	NO	NO	NO	NO	YES
Does the app use these 2 security precautions?					
Default is to authenticate the user with each use	NO	NO	NO	YES	NO
Works with password managers	YES	YES	YES	NO	YES

The current state of privacy laws in the United States leaves a patchwork of protections for an individual's personal information with more gaps than coverage. Further, health privacy laws that consumers have relied upon for decades to protect sensitive details about themselves do not extend to direct-to-consumer health

technology such as reproductive health apps. The bar is low. But as a purveyor of wellness, you should aim higher. To that end, we write to urge you to:

1. Only use collected data for the purpose of the health app;
2. Limit the data you collect to only information needed to operate the app;
3. Decline to share or sell user information;
4. Safely destroy collected data once it is no longer needed to operate the app;
5. Give consumers clear and concise information about what you do with their data and why.

Respecting your customers' privacy is a basic and achievable goal. A blueprint for doing so is available in the form of the Digital Standard, a set of benchmarks that companies can use to design digital products that are respectful of consumer privacy rights.<sup>iii</sup> Protecting app users' personal data is also a fundamental civil liberty concern. In the hands of unintended parties, consumer data has been used to create psychological profiles of voters for illicit political purposes<sup>iv</sup>; and enabled businesses to create alternative, nonevidence based and potentially discriminatory, credit scores based on consumers' digital footprint.<sup>v</sup>

Reproductive health apps such as yours must act fairly and transparently so consumers can make informed choices, not only in their care but also in the tools they use to manage their health. Over 22,000 consumers who signed a recent Consumer Reports petition agree. While lawmakers in Washington D.C. and in the states grapple with the right approach to legally secure consumer privacy, we turn to you to hold yourself to a higher standard so consumers can trust that the apps they use to care for themselves are not violating their privacy.

Signed,

Consumer Reports  
ACLU of Washington  
Center for Democracy and Technology  
Common Sense Media  
Digital Privacy Alliance  
Electronic Frontier Foundation  
HumanFirst.Tech  
National Partnership for Women & Families  
National Women's Law Center  
Norwegian Consumer Council  
Privacy Rights Clearinghouse

---

<sup>i</sup> Pew Research Survey, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, (November 15, 2019).

<sup>ii</sup> Donna Rosato, "What your period tracker app knows about you," Consumer Reports (January 16, 2020).

<sup>iii</sup> The Digital Standard was launched by Consumer Reports in 2017 in partnership with privacy and security experts. It is available at <https://www.thedigitalstandard.org/>.

<sup>iv</sup> Ahead of the 2016 presidential election, Cambridge Analytica acquired data on Facebook users through an online entertainment quiz, which was only completed by about 270,000 people but revealed data on 50 million individuals. This was a prominent example of how data collected through seemingly innocuous ways can be used for illicit purposes. Jerry Beilinson, "Facebook Data May Have Been Illicitly Used for Politics, and It Started With a Quiz", Consumer Reports (March 17, 2018).

<sup>v</sup> National Bureau of Economic Research, Working Paper: On the Rise of FinTechs – Credit Scoring Using Digital Footprints, (April 2018, Revised July 2018). This study raises the concern that the digital footprint may be used as a proxy for legally prohibited variables – such as race, color, gender, national origin, and religion – which can lead to discrimination.



January 29, 2020

Aidan Hughes, CEO

Digital Alchemy, parent company of My Calendar

15127 NE 24th Street, Ste 132






Redmond, WA 98052

Via email to: aidanh@digitalalchemy.us

To whom it may concern:

We the undersigned organizations reach out to urge you to take the lead in improving the privacy standard for health apps such as your own. Reproductive health apps are offered as an empowerment tool for consumers eager for power and agency over their health. Yet at the same time, many health apps do not have proper privacy standards in place, which can result in sensitive health data falling into the wrong hands. The vast majority of Americans report feeling as if they have little or no control over the data collected on them.<sup>i</sup> Users of reproductive health apps have reason to be wary.

There are very few legal privacy restrictions on app developers. That a company has free rein to collect, use, and share user data does not mean that they should – they absolutely should not. Fundamentally, consumers do not expect their intimate health details to be shared with research and advertising companies without their explicit and informed permission. Yet Consumer Reports identified privacy issues with each of the reproductive health apps it recently evaluated, as summarized in the excerpt below.<sup>ii</sup>

					
	BabyCenter	Clue	Flo	My Calendar	Ovia
Is the privacy policy easy to understand?	NO	YES	YES	NO	YES & NO
Can you use without sharing your name and email?	YES	NO	YES	NO	NO
Who does the app share your data with?					
Advertisers and marketers	YES	YES	YES	YES	YES
Health researchers, with your permission	NO	YES	YES	NO	YES
Insurers and employers via wellness programs	NO	NO	NO	NO	YES
Does the app use these 2 security precautions?					
Default is to authenticate the user with each use	NO	NO	NO	YES	NO
Works with password managers	YES	YES	YES	NO	YES

The current state of privacy laws in the United States leaves a patchwork of protections for an individual's personal information with more gaps than coverage. Further, health privacy laws that consumers have relied upon for decades to protect sensitive details about themselves do not extend to direct-to-consumer health

technology such as reproductive health apps. The bar is low. But as a purveyor of wellness, you should aim higher. To that end, we write to urge you to:

1. Only use collected data for the purpose of the health app;
2. Limit the data you collect to only information needed to operate the app;
3. Decline to share or sell user information;
4. Safely destroy collected data once it is no longer needed to operate the app;
5. Give consumers clear and concise information about what you do with their data and why.

Respecting your customers' privacy is a basic and achievable goal. A blueprint for doing so is available in the form of the Digital Standard, a set of benchmarks that companies can use to design digital products that are respectful of consumer privacy rights.<sup>iii</sup> Protecting app users' personal data is also a fundamental civil liberty concern. In the hands of unintended parties, consumer data has been used to create psychological profiles of voters for illicit political purposes<sup>iv</sup>; and enabled businesses to create alternative, nonevidence based and potentially discriminatory, credit scores based on consumers' digital footprint.<sup>v</sup>

Reproductive health apps such as yours must act fairly and transparently so consumers can make informed choices, not only in their care but also in the tools they use to manage their health. Over 22,000 consumers who signed a recent Consumer Reports petition agree. While lawmakers in Washington D.C. and in the states grapple with the right approach to legally secure consumer privacy, we turn to you to hold yourself to a higher standard so consumers can trust that the apps they use to care for themselves are not violating their privacy.

Signed,

Consumer Reports  
ACLU of Washington  
Center for Democracy and Technology  
Common Sense Media  
Digital Privacy Alliance  
Electronic Frontier Foundation  
HumanFirst.Tech  
National Partnership for Women & Families  
National Women's Law Center  
Norwegian Consumer Council  
Privacy Rights Clearinghouse

---

<sup>i</sup> Pew Research Survey, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, (November 15, 2019).

<sup>ii</sup> Donna Rosato, "What your period tracker app knows about you," Consumer Reports (January 16, 2020).

<sup>iii</sup> The Digital Standard was launched by Consumer Reports in 2017 in partnership with privacy and security experts. It is available at <https://www.thedigitalstandard.org/>.

<sup>iv</sup> Ahead of the 2016 presidential election, Cambridge Analytica acquired data on Facebook users through an online entertainment quiz, which was only completed by about 270,000 people but revealed data on 50 million individuals. This was a prominent example of how data collected through seemingly innocuous ways can be used for illicit purposes. Jerry Beilinson, "Facebook Data May Have Been Illicitly Used for Politics, and It Started With a Quiz", Consumer Reports (March 17, 2018).

<sup>v</sup> National Bureau of Economic Research, Working Paper: On the Rise of FinTechs – Credit Scoring Using Digital Footprints, (April 2018, Revised July 2018). This study raises the concern that the digital footprint may be used as a proxy for legally prohibited variables – such as race, color, gender, national origin, and religion – which can lead to discrimination.