epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

December 9, 2020

Honorlock, Inc.
2500 N Military Trail
Suite 322
Boca Raton, FL 33431

Dear Counsel:

We write in regard to Honorlock, Inc.'s provision of online test proctoring services. We represent the Electronic Privacy Information Center ("EPIC"), a public interest research center located in Washington, D.C., focused on emerging privacy and civil liberties issues. EPIC is one of the leading consumer protection organizations in the country specializing in privacy and data protection. EPIC has a long history of promoting transparency and accountability for information technology.[1] Our members include experts in law, technology, and public policy.

This letter serves as notice that EPIC has filed a Complaint and Request for Investigation, Injunction, and Other Relief with the Office of the Attorney General for the District of Columbia regarding Honorlock's online proctoring tools. As we set forth in the Complaint, Honorlock's excessive and unjustified collection of students' personal information (including biometric data) and reliance on opaque, unproven AI analysis to flag purported instances of cheating constitute unfair or deceptive trade practices under the D.C. Consumer Protection Procedures Act ("DCCPPA") and the Federal Trade Commission Act ("FTC Act"). This letter also serves as notice of EPIC's intent to bring an action against Honorlock for violations of the DCCPPA if Honorlock fails to promptly cure its unlawful trade practices.

In response to the COVID-19 pandemic, many educational institutions have implemented online test proctoring services as part of their remote learning arrangements.[2] But this rapid growth has brought renewed attention to the invasive nature of online proctoring systems. In order to meet their academic obligations, students must increasingly agree to compulsory collection of biometric

[1] *See* EPIC, *Algorithmic Transparency* (2020), https://www.epic.org/algorithmic-transparency/; EPIC, *Algorithms in the Criminal Justice System* (2020), https://www.epic.org/algorithmic-transparency/crim-justice/; Complaint of EPIC, *In re Airbnb* (Feb. 26, 2020); Petition of EPIC, *In re Petition for Rulemaking Concerning Use of Artificial Intelligence in Commerce* (Feb. 2020), https://epic.org/privacy/ftc/ai/epic-ai-rulemaking-petition/; Complaint of EPIC, *In re HireVue* (Nov. 6, 2019), https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf; Comments of EPIC, *Consumer Welfare Implications Associated with the Use of Algorithmic Decision Tools, Artificial Intelligence, and Predictive Analytics*, Fed. Trade Comm'n (Aug. 20, 2018), https://epic.org/apa/comments/EPIC-FTC-Algorithmic-Transparency-Aug-20-2018.pdf.

[2] Drew Harwell, *Mass School Closures in the Wake of the Coronavirus Are Driving a New Wave of Student Surveillance*, Wash. Post (Apr. 1, 2020), https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/; *see also* Shea Swauger, *Software that Monitors Students During Tests Perpetuates Inequality and Violates Their Privacy*, MIT Tech. Rev. (Aug. 7, 2020), https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/.

and other sensitive personal data; audio and video surveillance of their intimate spaces; and opaque AI analysis of their movements, facial expressions, and keystrokes.

We are aware that Honorlock uses an in-browser extension to record and review students during exams and employs AI to monitor exam sessions and generate incident reports.[3] Honorlock states that it collects video and audio recordings of test-takers, monitors desktop activity, and tracks webpages visited by each student during an exam.[4] We are also aware that Honorlock uses a combination of AI proctoring and live proctoring. Honorlock states that its AI monitors students and will trigger a live proctor to drop in on the student's feed if the AI "senses that something is wrong."[5] For example, Honorlock states that its AI may trigger a live proctor when a student diverts their eyes from the screen or gets up from their desk.[6]

A student enrolled at an institution which uses Honorlock has no choice but to allow the collection of their personal information and to submit to video monitoring and AI analysis in order to complete their required examinations. Yet Honorlock has failed to establish a legitimate need for collecting such a vast array of personal data; Honorlock has failed to fully disclose to students the logic, factors, and determinations of its AI; and Honorlock has failed to identify any benefits to consumers or competition that would outweigh the privacy and other harms suffered by students.

Honorlock has also made misleading statements concerning its use of facial recognition software. Although Honorlock claims that it does not employ facial recognition,[7] its proctoring systems use tools that meet the FTC's definition of facial recognition. Honorlock contends that, rather than using facial recognition, it employs "facial detection" which "only detects that there is a clear human face in the webcam."[8] But as the FTC explained in a 2012 report, facial detection *is* facial recognition—not a separate technology. As the FTC wrote: "[C]ompanies are deploying facial recognition technologies in a wide array of contexts, reflecting a spectrum of increasing technological sophistication. *At the simplest level, the technology can be used for facial detection*; that is, merely to detect and locate a face in a photo."[9]

The above-described business practices constitute violations of the DCCPPA, including but not limited to sections 28–3904 (unfair or deceptive trade practices generally), 28-3904(e) (misrepresentation as to a material fact), and 28-3904(f) (failure to state a material fact). Accordingly, EPIC and affected consumers are entitled to injunctive and monetary relief, in addition to any enforcement action taken against Honorlock by the Attorney General for the District of Columbia.[10] These practices also constitute violations of Section 5 of the FTC Act,[11] exposing Honorlock to potential FTC enforcement proceedings.

---

[3] *Honorlock*, Honorlock (2020), https://honorlock.com/.
[4] *Honorlock Protects Student Privacy*, Honorlock (2020), https://honorlock.com/studentprivacy/.
[5] *Frequently Asked Questions*, Honorlock (2020), https://honorlock.com/students/#faq.
[6] *Id.*
[7] *Honorlock Protects Student Privacy*, Honorlock (2020), https://honorlock.com/studentprivacy/#faq.
[8] *Id.*
[9] *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Fed. Trade Comm'n (Oct. 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf (emphasis added).
[10] D.C. Code § 28–3905(i)(3)(B).
[11] 15 U.S.C. § 45(a).

In order to avoid litigation between EPIC and Honorlock and to protect the privacy of Honorlock test-takers, EPIC hereby demands that Honorlock commit in writing to:

1. Strictly limit its collection of students' personal and biometric information;
2. Create, maintain, and publish a detailed log of what types of personal information Honorlock collects from test-takers, how Honorlock uses such data, and how long Honorlock retains such data;
3. Refrain from transferring or providing third parties access to personal data collected from test-takers, including images of students;
4. Provide students with access, correction, and deletion rights with respect to their own data;
5. Make available to students the factors, logic, and determinations of the AI system(s) used to produce assessments of test-takers;
6. Comply fully with the Organisation for Economic Co-operation and Development ("OECD") Principles on Artificial Intelligence[12] and Universal Guidelines for Artificial Intelligence;[13] and
7. Submit to an annual audit by an independent third party of Honorlock's privacy, data collection, and AI practices, the results of which shall be publicly reported.

If Honorlock does not comply with the requests set forth in this letter, EPIC reserves all rights and remedies, including legal action. Accordingly, EPIC requests that Honorlock takes steps to preserve all records, communications, and other evidence potentially relevant to such litigation, including but not limited to evidence concerning the collection, use, retention, and disclosure of Honorlock user data and the operation of its AI system(s) used to evaluate test-takers for signs of academic dishonesty.

EPIC would prefer to resolve this matter amicably, and we look forward to your response by December 18, 2020. This letter is not a recitation of all of the facts pertaining to this matter or all of EPIC's possible claims. Accordingly, EPIC is not waiving any of its rights and remedies, all of which EPIC expressly reserves.

/s/ Alan Butler
Alan Butler
EPIC Interim Executive Director
and General Counsel
butler@epic.org

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Interim Associate Director
and Policy Director
fitzgerald@epic.org

/s/ John Davisson
John Davisson
EPIC Senior Counsel
davisson@epic.org

/s/ Sara Geoghegan
Sara Geoghegan
EPIC Law Fellow
geoghegan@epic.org

[12] *Recommendation of the Council on Artificial Intelligence*, OECD (May 21, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
[13] *Universal Guidelines for Artificial Intelligence*, The Public Voice (Oct. 23, 2018), https://thepublicvoice.org/ai-universal-guidelines/.