152 3187

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of	)	
	)	
IOActive, Inc.,	)	
a corporation.	)	
	)	
	)	**DOCKET NO. C-4542**
	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that IOActive, Inc., a corporation, has violated the Federal Trade Commission Act ("FTC Act"), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent IOActive, Inc. is a Washington corporation with its principal office or place of business at 701 5th Avenue, Suite 6850, Seattle, Washington.

2. Respondent describes itself as providing security consulting services.

3. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act.

4. Respondent has set forth on its website, www.ioactive.com, privacy policy statements about its practices, including statements related to its participation in the Safe Harbor privacy framework agreed upon by the U.S. and the European Union ("the U.S.-EU Safe Harbor Framework").

The Safe Harbor Framework

5. The U.S.-EU Safe Harbor Framework provides a method for U.S. companies to transfer personal data outside of Europe that is consistent with the requirements of the European Union Directive on Data Protection ("Directive"). Enacted in 1995, the Directive sets forth European Union ("EU") requirements for privacy and the protection of personal data. Among other things, it requires EU Member States to implement legislation that prohibits the transfer of personal data outside the EU, with exceptions, unless the European Commission ("EC") has made a determination that the recipient jurisdiction's

laws ensure the protection of such personal data. This determination is referred to commonly as meeting the EU's "adequacy" standard.

6. To satisfy the EU adequacy standard for certain commercial transfers, the U.S. Department of Commerce ("Commerce") and the EC negotiated the U.S.-EU Safe Harbor Framework, which went into effect in 2000. The U.S.-EU Safe Harbor Framework allows U.S. companies to transfer personal data lawfully from the EU. To join the U.S.-EU Safe Harbor Framework, a company must self-certify to Commerce that it complies with seven principles and related requirements that have been deemed to meet the EU's adequacy standard.

7. Companies under the jurisdiction of the U.S. Federal Trade Commission ("FTC"), as well as the U.S. Department of Transportation, are eligible to join the U.S.-EU Safe Harbor Framework. A company under the FTC's jurisdiction that claims it has self-certified to the Safe Harbor principles, but failed to self-certify to Commerce, may be subject to an enforcement action based on the FTC's deception authority under Section 5 of the FTC Act.

8. Commerce maintains a public website, www.export.gov/safeharbor, where it posts the names of companies that have self-certified to the U.S.-EU Safe Harbor Framework. The listing of companies indicates whether their self-certification is "current" or "not current" and a date when recertification is due. Companies are required to re-certify every year in order to retain their status as "current" members of the U.S.-EU Safe Harbor Framework.

The U.S.-EU Safe Harbor Framework Certification Mark

9. In 2008, Commerce developed the U.S.-EU Safe Harbor Framework Certification Mark ("the mark"). Upon request, Commerce provides the mark to those organizations that maintain a "current" self-certification to the U.S.-EU Safe Harbor Framework. In addition, Commerce has established certain rules for using the mark, such as requirements relating to the mark's placement on a website and the inclusion of a link to www.export.gov/safeharbor. The mark appears as follows:

Violations of Section 5 of the FTC Act

Misrepresentations Regarding Safe Harbor Participation

10. In May 2009, respondent submitted to Commerce a self-certification of compliance with the U.S.-EU Safe Harbor Framework, which is publicly available at the www.export.gov/safeharbor website.

11. In May 2012, respondent did not renew its self-certification to the U.S.-EU Safe Harbor Framework, and Commerce subsequently updated respondent's status to "not current" on its public website.

12. Since at least May 2009 until May 2015, respondent disseminated or caused to be disseminated privacy policies and statements on its website, www.ioactive.com/privacy-policy.html, including but not limited to, the following privacy policy statement and display of the mark:

> **Safe Harbor Compliance**
>
> The company complies with the U.S.-EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. The company has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view the company's certification, please visit the Safe Harbor website.
>
> We self-certify compliance with
>
> 
>

13. Through the means described in Paragraph 12, respondent represented, expressly or by implication, that it was a current participant in the U.S.-EU Safe Harbor Framework.

14. In truth and in fact, beginning in 2012, respondent was not a current participant in the U.S.-EU Safe Harbor Framework. Therefore, the representation set forth in Paragraph 13 is false and misleading.

15. The acts and practices of respondent as alleged in this complaint constitute deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this twenty-ninth day of September 2015, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary

SEAL