Federal Trade Commission: Workshop on Bringing Dark Patterns to Light

Comments of BSA | The Software Alliance

BSA | The Software Alliance welcomes the opportunity to provide these comments in connection with the public workshop by the Federal Trade Commission ("FTC" or "Commission") on bringing dark patterns to light. The workshop is a part of the FTC's important efforts to highlight concerns around dark patterns. BSA applauds the Commission's work to protect consumers and to bring together researchers, legal experts, consumer advocates, and industry professionals to examine what dark patterns are and how they affect both consumers and the marketplace.

BSA is the leading advocate for the global software industry before governments and in the international marketplace.[1] Our members are enterprise software companies that create the business-to-businesses technology products and services that power other companies. BSA members offer tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations, and their business models do not depend on monetizing users' data.

BSA strongly believes that consumers should not be surprised about how their personal data is used – and they should not be tricked or misled by dark patterns. Our comments focus on two aspects of dark patterns. *First*, we recognize the significant concerns around dark patterns raised by both the FTC and by consumer advocates. *Second*, we focus on how a federal privacy law can help to eliminate the use of dark patterns, by guaranteeing important rights for consumers and requiring businesses to use consumers' personal data in ways that consumers expect.

I. Dark Patterns Harm Consumers

Consumers should not be misled, tricked, or surprised about the products and services they purchase or about how their personal data is used. We appreciate the serious concerns raised by the FTC and by consumer advocates about deceptive practices that mislead consumers into making purchases they otherwise would not, or that misrepresent the quality, origin, design, or durability of a product, or that

[1] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

deceive consumers into giving away their personal data. Put simply, responsible companies should not condone the use of dark patterns — and should not create business models that rely on misleading consumers.

Online technologies should be designed to serve consumers. When BSA companies make technology products and services to be used in the business-to-business environment, they are designed to be clearly understood, easy to navigate, and helpful to the businesses that rely on those technologies to store, send, and process their information. Consumer-facing products should similarly be designed with consumers in mind. It should be easy for individuals to use technology to communicate with their friends and family, to buy products and services online, and to navigate the digital environment.

We agree with the workshop participants who recognize that dark patterns can be difficult to define – and recognize the careful attention that must be given to defining dark patterns in any future FTC guidance. At the same time, the deceptive tactics at the heart of dark patterns have long been a focus of enforcement actions by not only the FTC but also by state attorneys general. We also recognize that dark patterns are proliferating despite these active enforcement efforts. In many cases, though, because dark patterns are inherently deceptive, consumers may not be in a position to alert authorities about these practices. Dark patterns not only cost consumers money, by tricking them into paying for unnecessary services or into agreeing to pay inflated prices, but they can increase consumers' frustration with technologies and undermine their trust in digital services. Educating consumers about dark patterns is not enough to address these issues. Rather, the FTC must continue its active enforcement in this area – and would be aided by new tools and authorities in a federal privacy law.

II. Federal Privacy Legislation Can Help Eliminate Dark Patterns

A federal privacy law can help eliminate dark patterns. BSA strongly supports a federal privacy law, which we believe should focus on three key components: (1) establishing consumer rights over their personal data, including rights to access, correct, and delete their personal data, (2) creating meaningful obligations for businesses to ensure they handle personal data in ways that consumers expect, and (3) providing strong enforcement, including not only by the FTC but by all state attorneys general.

We believe a federal privacy law can help eliminate dark patterns in three ways:

1. ***A federal privacy law should build on state laws, including those addressing dark patterns.*** Congress should build on the privacy laws enacted in states like California and Virginia to create comprehensive privacy legislation that protects consumers nationwide.[2] States considering their own comprehensive consumer privacy bills have already begun addressing dark patterns. In California, voters approved a ballot initiative last fall that makes clear dark patterns cannot be used to obtain a consumer's consent.[3] In regulations under the California Consumer Privacy Act, the California Attorney prohibited certain types of dark patterns, including the use of double-

[2] *See, e.g.*, BSA | The Software Alliance, Comprehensive Federal Privacy Legislation Can Build on State Privacy Laws, available at https://www.bsa.org/files/policy-filings/04212021fedprivacylegislation.pdf.

[3] *See* California Privacy Rights Act, Cal. Civ. Code 1798.140(h). California's new privacy regulator will also be tasked with further defining dark patterns, which are described as a "user interface designed or manipulated with the substantial effect of impairing user autonomy, decisionmaking, or choice, as further defined by regulation."

negatives in consent requests.[4] A bill passed by the Washington State Senate would have similarly prohibited consent obtained through dark patterns.[5] Congress should build on these important conversations at the state level to ensure consumers nationwide are protected against dark patterns.

2. ***A federal privacy law can provide new authorities for the FTC to take action against companies that engage in privacy violations such as using dark patterns.*** Effective enforcement is important to protecting consumers' privacy, ensuring that organizations meet their commitments and legal obligations, and deterring potential violations. Federal law already prohibits many dark patterns, including through the ban on deceptive and unfair acts and practices contained in Section 5 of the FTC Act. We believe that a comprehensive federal privacy law should give the FTC new authorities to enforce privacy violations. Specifically, BSA supports a federal privacy law that provides the FTC with new tools including targeted rulemaking authority, the ability to fine first-time violators, and additional funding and staff. Moreover, the FTC should not be the only agency enforcing a federal privacy law. State attorneys general should also be empowered to enforce a federal privacy law, which will complement their longstanding privacy enforcement efforts at the state level.

3. ***A federal privacy law should ensure that any consent requirements are strong and meaningful***. Dark patterns undermine efforts by responsible companies to seek consumers' consent, by using deceptive user interfaces and intentionally-confusing consent requests. In our view, a federal privacy law should place a range of obligations on companies to ensure consumers' personal data is used in ways that consumers expect. Those obligations should include strong consent requirements for the collection of sensitive personal information like precise geometric information, financial account information, or health information. Such requirements can help to ensure each consent request is meaningful to consumers, and can help to avoid frequent consent requests that fatigue consumers and dilute the effectiveness of each request. Those consent requirements should be combined with other guardrails – beyond consent – such as data minimization and purpose specification, which can further safeguard consumers' personal data. A federal privacy law should combine these obligations for companies that collect and use consumers' personal data, rather than relying on consent alone to protect consumers.

III. Conclusion

BSA applauds the FTC's leadership on consumer privacy and its willingness to address emerging issues that can harm consumers and undermine responsible uses of technology. We would welcome the opportunity to discuss these issues with you in more detail.

[4] *See* California Consumer Privacy Act Regulations, § 999.315(h)(2) (March. 31, 2021), available at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-add-adm.pdf.
[5] *See* Washington Privacy Act, SB 5062 (second substitute) (not enacted) Sec. 101(6), available at http://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5062-S2.pdf.