

**CONSUMER PRIVACY BILL OF RIGHTS**

<p align="center"><b><u>ISSUES</u></b></p> <p align="center"><b><u>USE CASES</u></b></p>	<p><b>INDIVIDUAL CONTROL:</b> Consumers have a right to exercise control over what personal data companies collect from them and how they use it.<sup>1</sup></p>	<p><b>TRANSPARENCY:</b> Consumers have a right to easily understandable and accessible information about privacy and security practices.<sup>2</sup></p>	<p><b>RESPECT FOR CONTEXT:</b> Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.<sup>3</sup></p>	<p><b>SECURITY:</b> Consumers have a right to secure and responsible handling of personal data.<sup>4</sup></p>	<p><b>ACCESS AND ACCURACY:</b> Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.<sup>5</sup></p>	<p><b>FOCUSED COLLECTION:</b> Consumers have a right to reasonable limits on the personal data that companies collect and retain.<sup>6</sup></p>	<p><b>ACCOUNTABILITY:</b> Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.<sup>7</sup></p>	<p><b>FIRST AMENDMENT:</b></p>
<p><b><u>Use Case #1</u></b></p> <p>A pro-pot legalization march is held in Sacramento, CA within full view of dozens of public and private surveillance cameras. Corporations use facial recognition technology to sell pot tours to Colorado and other products that they have found to be linked to favorable views on marijuana. Law enforcement agencies seek to obtain facial recognition data from companies to identify law breakers.</p>								

<p><b><u>Use Case #4</u></b></p> <p>Photos are taken of people in casinos and matched with photos from social networking sites for purposes of identifying them and selling that information to data brokers who would put them on lists of ‘people who like to take chances.’ These lists could then be used to solicit them for bogus sweepstakes and lotteries, investments, and business opportunities.</p>								
<p><b><u>Use Case # 13</u></b></p> <p>Facebook, Google, and others are working on facial recognition research to expand application capabilities, including for the consumer sector. This brief case study will identify the major research initiatives, discuss current projects, and address preliminary consumer and privacy implications.</p>								
<p><b><u>Use Case #22</u></b></p> <p>A National Bank’s ATM uses multi-factor authentication to prevent fraudulent</p>								

<p>withdrawals, including facial recognition matched to stored images on the bank's computers. National Bank performs the authentication when their customers use National Bank ATMs and when their customers use non-National Bank ATMs.</p>								

<sup>1</sup> Elaboration in the White House Consumer Privacy Bill of Rights: “Companies should provide consumers appropriate control over the personal data that consumers share with others and over how companies collect, use, or disclose personal data. Companies should enable these choices by providing consumers with easily used and accessible mechanisms that reflect the scale, scope, and sensitivity of the personal data that they collect, use, or disclose, as well as the sensitivity of the uses they make of personal data. Companies should offer consumers clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use, and disclosure. Companies should offer consumers means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place.”

<sup>2</sup> Elaboration in the White House Consumer Privacy Bill of Rights: “At times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks and the ability to exercise Individual Control, companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties.”

<sup>3</sup> Elaboration in the White House Consumer Privacy Bill of Rights: “Companies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise. If companies will use or disclose personal data for other purposes, they should provide heightened Transparency and Individual Control by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection. If, subsequent to collection, companies decide to use or disclose personal data for purposes that are inconsistent with the context in which the data was disclosed, they must provide heightened measures of Transparency and Individual Choice. Finally, the age and familiarity with technology of consumers who engage with a company are important elements of context. Companies should fulfill the obligations under this principle in ways that are appropriate for the age and sophistication of consumers. In particular, the principles in the Consumer Privacy Bill of Rights may require greater protections for personal data obtained from children and teenagers than for adults.”

<sup>4</sup> Elaboration in the White House Consumer Privacy Bill of Rights: “Companies should assess the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure.”

---

<sup>5</sup> Elaboration in the White House Consumer Privacy Bill of Rights: “Companies should use reasonable measures to ensure they maintain accurate personal data. Companies also should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation. Companies that handle personal data should construe this principle in a manner consistent with freedom of expression and freedom of the press. In determining what measures they may use to maintain accuracy and to provide access, correction, deletion, or suppression capabilities to consumers, companies may also consider the scale, scope, and sensitivity of the personal data that they collect or maintain and the likelihood that its use may expose consumers to financial, physical, or other material harm.”

<sup>6</sup> Elaboration in the White House Consumer Privacy Bill of Rights: “Companies should collect only as much personal data as they need to accomplish purposes specified under the Respect for Context principle. Companies should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise.”

<sup>7</sup> Elaboration in the White House Consumer Privacy Bill of Rights: “Companies should be accountable to enforcement authorities and consumers for adhering to these principles. Companies also should hold employees responsible for adhering to these principles. To achieve this end, companies should train their employees as appropriate to handle personal data consistently with these principles and regularly evaluate their performance in this regard. Where appropriate, companies should conduct full audits. Companies that disclose personal data to third parties should at a minimum ensure that the recipients are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise.”