While most previous keystroke biometric work dealt with short input like passwords, we focused on long-text input for applications such as identifying perpetrators of inappropriate e-mail or fraudulent Internet activity. A Java applet collected raw keystroke data over the Internet, appropriate long-text-input features were extracted, and a pattern classifier made identification decisions. Initial experiments focused on the system’s usability under ideal conditions: copy task, long-text input (600 characters), same keyboard for enrollment and testing, and subjects aware of the nature of the study and instructed to type naturally. Essentially 100% identification accuracy was achieved on 10 subjects typing the same text, and this accuracy decreased in going to 30 subjects, on copying different testing texts, and on progressively reducing the length of the testing text. Subsequent experiments focused on measuring accuracy degradation under less ideal conditions: arbitrary text input (non-copy task), laptop versus desktop keyboards, and naïve users (unaware their data was captured for identification purposes). In summary, we found the keystroke biometric effective for identifying up to 30 aware or naïve users inputting arbitrary text under the following conditions: sufficient training and testing text length (600 characters), sufficient number of enrollment samples, and same keyboard type used for enrollment and testing.