**TEXT 6**

**Match the following words with their definitions**

|  |  |
| --- | --- |
| 1.to extend | A used when giving your opinion to say that there are good reasons why smth. might be true |
| 2.stringent, severe | B small and not very important or serious |
| 3.violation | C old-fashioned |
| 4.arguably | D to continue for a longer period of time/particular distance/over a particular area  |
| 5.to abuse | E the act of ending smth., or the end of smth.  |
| 6.minor | F unclear, confusing, or not certain, especially because it can be understood in more than one way |
| 7.felony | G to be equal to (in quantity or in meaning) |
| 8.termination | H expressing a strongly unfavourable judgement |
| 9.mischief | I very unkind and cruel, and deliberately behaving in a way that is likely to upset or hurt someone |
| 10.ambiguous | J a serious crime such as murder |
| 11.dated | K to deliberately use smth. for the wrong purpose or for your own advantage |
| 12.benign | L knowledge or understanding of a particular subject or situation |
| 13.malicious | M an action that breaks a law, agreement, principle etc. |
| 14.to amend | N kind and gentle |
| 15.to amount to | O to correct or make small changes to smth. that is written or spoken |
| 16.awareness | P damage or harm that is done to someone or to their property  |

**It’s Time to Reform the Computer Fraud and Abuse Act**

A bill working its way through Congress is an opportunity to update an unfair, outmoded cybersecurity law

By [James Hendler](http://www.scientificamerican.com/author.cfm?id=35240)

**1** This year the U.S. Congress is considering changes to the [Computer Fraud and Abuse Act (CFAA)](https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_%28CFAA%29), the primary law that governs cyber crime and fraud on the [Internet](http://www.scientificamerican.com/topic.cfm?id=internet). The act, originally passed in 1986, was aimed at providing a measure of [security](http://www.scientificamerican.com/topic.cfm?id=security) for computers against unauthorized access to large, time-shared computers. Back then the perceived threat was serious computer hacking—people breaking into the banking system or the nuclear control system (remember the movie *War Games*?). The act has been extended many times since, including as part of the post-9/11 Patriot Act. Now, in response to a reported increase in cyber attacks coming from abroad, many members of Congress want to again expand the CFAA, adding to the stringency of the law with the intent of further protecting America’s computing resources.

**2** One bill, however—“[Aaron’s Law](http://www.lofgren.house.gov/images/stories/pdf/aarons%20law%20-%20lofgren%20-%20061913.pdf),” introduced in June by Rep. Zoe Lofgren (D–Calif.) and Sen. Ron Wyden (D–Ore.)—would appear to go in the other direction. Aaron’s law removes some computer activities from coverage under the act and limits the prosecution of certain CFAA violations. And although that might seem counterintuitive in a time of increased cyber crime, it is in fact a necessary reform to a deeply flawed and outdated law.

**3** Aaron’s law is named for [Aaron Swartz](http://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html?pagewanted=all&_r=0" \t "_blank), the Internet activist who committed suicide in January. Before his death at age 26**,** Aaron contributed much to society, both technically and politically. He helped develop the RSS syndication format used for Web-based news feeds, the social news site Reddit and the Creative Commons codes now used to help promote the online sharing of Web content. Politically, he was well known for his role in founding the group Demand Progress, one of the more effective voices against legislation that many believe would have significantly limited online free speech and innovation. One of his causes was “Open Data.” He realized that sitting in many computers was a lot of inaccessible information that, in principle, anyone should be able to access. He was committed to taking publicly funded data—including the results of government-funded scientific research—and making it available on the Web for easy access.

**4** That may have been what he was trying to achieve when, in January 2011, he downloaded a large number of articles from the academic-document archive JSTOR onto his laptop.Aaron had a JSTOR account, allowing him access to the work, but he arguably abused that access by setting up a computer at Massachusetts Institute of Technology and downloading articles in bulk over a period of weeks. He was originally arrested on a minor charge, and JSTOR decided not to pursue the case. Unfortunately, federal prosecutors did not drop the charges. Under the CFAA, Aaron was charged with 11 felony violations and faced up to 35 years in prison. Two years later, as the trial approached, he hanged himself in his Brooklyn apartment

**5** Swartz is not the only victim of apparent overprosecution under the CFAA. Keith Downey, a 28-year-old programmer from Florida, is accused of [attacking PayPal’s server](http://www.abajournal.com/magazine/article/hackers_hell_many_want_to_narrow_the_computer_fraud_and_abuse_act/%22%20%5Ct%20%22_blank) to protest its termination of a donation page for Wikileaks. Whether this was mischief, crime or civil disobedience seems an appropriate question for the courts to address. But the 15-year prison sentence Downey currently faces is out of proportion. To put this in perspective, 15 years is the same sentence recently given to one criminal convicted of child sex abuse and another of gang-related homicide.

**6** In another high-profile case, 27-year-old Andrew Auernheimer was [convicted](https://www.eff.org/cases/us-v-auernheimer%22%20%5Ct%20%22_blank) under CFAA for attacking AT&T servers and turning over illegally obtained information about iPad users to the gossip site Gawker.com. (Auernheimer and another man, Daniel Spitler, who was also charged in the case, claimed that their goal was to show AT&T that iPad-generated information was not secure in their system.) Auernheimer was threatened with long jail time and eventually pleaded to a 41-month sentence, the same punishment a convicted child pornographer received that month. One can argue about Auernheimer’s motivation, and the blogosphere is full of discussion about whether he should be considered a whistle-blower or a criminal hacker. But either way, the severity of the punishment seems unduly harsh.

The recent movie version of Victor Hugo’s *Les Mis*é*rables* reminded us of the story of Jean Valjean, who was thrown in prison for many years for stealing a loaf of bread. There are still parts of the world in which thieves are punished by having their hands cut off, or where offenses against a religious belief are punishable by death. These stories offend our notions of jurisprudence; in America we have been brought up to understand that a punishment should fit the crime.

**7** Yet the CFAA is written is such an ambiguous and dated way that the punishments it prescribes are often wildly disproportionate to the crime. For example, the CFAA allows prosecutors to pursue the same draconian measures—with punishments ranging from five to 15 years per charge—for acts as benign as violating the terms of a vendor’s service agreements and those as malicious as a concerted effort to break into a computer and steal credit card numbers. The CFAA violations that Swartz, Downey and Auernheimer were charged with were hardly major acts of computer terrorism, yet the law treated them as such.

Aaron’s law would amend the CFAA to clarify the intent of the act. In particular, the bill clarifies the definitions of damages caused by computer crimes, makes penalties proportional to those damages, and disallows the stacking of duplicate charges, which is allowed under the current law. The modified CFAA would more clearly differentiate between serious computer fraud and minor violations such as terms-of-service violations and improper employee behavior without criminal intent. This long-overdue reworking of the CFAA is a first step in the direction of fixing a bad bill.

**8** Computer crime is becoming an increasing danger to our society, and we cannot ignore the need for federal and international laws that allow strong penalties for serious online offenses. But these laws must be written in a way that does not harshly prosecute those whose cyber acts amount to the metaphorical theft of bread. Not only would this be a step toward basic fairness, but it would also enable law enforcement to focus on serious computer attacks rather than nuisance events.

**9** In the long term, changes to the CFAA could deliver another important benefit. Just as overall crime goes down when we lock our doors and cars, so too will computer crime go down when the public more widely provides basic [security](http://www.scientificamerican.com/topic.cfm?id=security) on their own machines. As Aaron’s law shifts law enforcement’s focus to major crimes, computer users may start to realize that rather than counting on the FBI to protect them, they need to install local, simple solutions. In that way, Aaron’s law would not only bring an outdated law into the 21st century, it could also lead to a growing awareness that the best enforcement against computer crime starts in one’s own home.

**In the following passages of the article find English equivalents of Russian words and word combinations**

**Pas.1**

1.несанкционированный доступ

**Pas.3**

1.покончить жизнь самоубийством

2.лента новостей

**Pas.4**

1.снять обвинение

**Pas.5**

1.гражданское неповиновение

2.несоразмерный

3.объективно оценивать

**Pas.6**

1.доносчик, осведомитель

2.чрезмерно суровый

**Pas.7**

1.сложение наказаний по совокупности преступлений

2.давно назревшая переработка

**Pas.8**

1.обеспечение правопорядка

**Pas.9**

1.в долгосрочном плане

**Answer the following questions**

1.Why does the US Congress want to reform the Computer Fraud and Abuse Act?

2.What was Aaron Swartz committed to do?

3.What happened to him when he was arrested?

4.What is common for cases mentioned in the article?

5.What is the main notion of jurisprudence?

6.What does the bill “Aaron’s Law” claim and clarify?

7.What should law enforcement in the field of computer crimes focus on?

8.How can ordinary people contribute to decreasing computer crimes?