BSA Response to the Business Innovation & Skills Committee on the Draft Consumer Rights Bill

September 2013

BSA | The Software Alliance (BSA)[1] appreciates the opportunity to respond to the UK Parliament's Business, Innovation and Skills Committee on the UK Government's draft Consumer Rights Bill. BSA members have a long-standing presence and history of innovation in the UK market, and provide a wide range of software and digital services to consumers across the UK. Our members' products and services span a wide range, including software (including enterprise software, general consumer productivity and language software, security software, apps, games, etc.), cloud services (including free online communication services such as VoIP, free email accounts, cloud storage and photo hosting, as well as digital download services), operating systems, and consumer portable and computer devices.

Our members have been actively involved for many years in issues relating to the digital economy, including how consumer rights should be extended to software and other digital services. We support the aim of creating simpler, clearer consumer rights legislation, and we have worked extensively with the European Union institutions, as well as with national EU Member State governments, to help develop the Consumer Rights Directive. We believe the Directive's harmonization of consumer law across the EU will help to create a more unified digital market that will spur further growth in our industry.

Our industry has a number of comments and concerns about the draft Consumer Rights Bill (draft CR Bill) that we would like to share with the Committee. Moreover, as it will not be possible to exclude or restrict the liabilities resulting from the draft CR Bill (Clause 49 of the current draft), we believe our comments, many of which have been made before, need to be taken into account. The alternative would be to impose unclear and unavoidable liabilities on our industry, potentially damaging growth in the sector in the UK.

"Digital content" is fundamentally not the same as physical goods, so different rules are needed. Our most important concern is a fundamental one. In Chapter 3, the CR Bill sets out

[1] BSA |The Software Alliance is the leading advocate for the global software industry before governments and in the international marketplace. With offices in Brussels, London, and Munich, BSA is active across the European Union and in more than seventy countries around the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include: Adobe, Apple, Autodata, Autodesk, AVG, Bentley Systems, CA technologies, CNC Software, Dell, IBM, Intel, Intuit, McAfee, Microsoft, Minitab, Oracle, PTC, Rosetta Stone, Siemens PLM Software, Symantec, Tekla, and The Mathworks.

consumer rights and remedies relating to digital content, but in many cases the concepts implemented by these provisions are simply transpositions of pre-existing rights and remedies in consumer sale of goods law. The problem is that these pre-digital concepts were created many years ago, in a world without software, and do not match up well with the concept of "digital content", which is very different from a physical good.

A key point is that physical goods are static and do not change, but the same is not true for certain types of digital content, such as security software. Many types of software are constantly updated, and develop, often in complex ways, over time. What is more, digital content must always rely on a consumer electronic device and other software to operate as intended, and so exist in a rapidly changing ecosystem, whereas physical goods are provided separately and function independently from other physical goods.

These differences create real uncertainties when applying traditional rules to the provision of digital content. For example, it is far from clear what a "fault" would look like in digital content. Many security breaches are not a result of vulnerable software or questionable coding, but rather of incorrect use, unpatched software or malware introduced. Software functionality can be impaired by user unawareness, incorrect installation or non-application of security updates, the use of infected USB devices, the use of insecure passwords, opening unsolicited e-mails, etc. In many circumstances, without months of research and dedicated investment, consumers and software developers may both be unable to identify why or how certain "faults" arise.

The current draft CR Bill does not take these types of complexity into account, nor does it account for the wide-ranging differences between types of digital content (i.e., software, digital music or films, digital services, etc.). If the draft CR Bill were enacted without more clarifications, consumers and industry would face confusion. We provide further in-depth examples of our concerns relating to Chapter 3 of the draft CR Bill, and to specific clauses of that Chapter, below:

- **The requirement that digital content be free from "minor defects" (Clause 36) is too broad, and is unfair to some software developers.** Clause 36(3) clarifies that the digital content is required to be "[free] from minor defects" in order to be of satisfactory quality. This requirement is unrealistic for software. Because software is very complex, and because it is developed rapidly, it is impossible to eliminate minor bugs and errors from software, and although these bugs do not normally impair main functionalities and usage, they could arguably be seen as "minor defects". These bugs are not normally known to software developers on release, and are often the result of complex interactions between hardware, other third party software, drivers, operating systems, and other factors. Once identified, they are often fixed in subsequent releases, but the "fixability" of each bug varies, as does the number of affected consumers. Requiring software to be provided without any of these minor defects is simply not technologically possible.

- **The requirement that digital content be "as described" (Clause 38) does not take into account how software develops and changes over time**. Clause 38 requires that digital content, including software, be provided to consumers as it has been described. Many types of software, for example security software, needs to be updated regularly,

and this process may mean that a specific functionality is removed. Updates may sometimes remove functionalities that have been discovered to be vulnerable to cyber-attacks and viruses, for example. In another scenario, some online games, which require dedicated servers to host, lose popularity over time, and online multiplayer functionality is ended (although the game remains playable in single player mode exactly as it did before). Patches perform many different purposes, but even when functionalities are removed, it is often in order to ensure that purchased software remains of high quality over time.

This clause should therefore be amended to take into account that many types of software do, and should, evolve over time. Requiring software to remain "as described" will only stifle innovation and prevent companies from taking risks that ultimately benefit consumers, with new functions and features.

- **The requirement that digital content be "repaired or replaced" (Clause 45) if it is not of satisfactory quality lacks clarity in the case of software**. Unfortunately, threats change over time. The result is that a "repair" that fixes one version of a threat might not fix another version, and may only be able to stop a threat by removing or disabling existing software functionality. In these cases, it is not clear whether or not the "repair" obligation has been satisfied. A further complexity is that software is often upgraded *en masse* – a software developer creates an update, and then uses a pre-designed functionality to update *all* installed versions of the software at once. This means that some customers, who may not have experienced a problem with their previous version of the software, suddenly find that another customer's exercise of their right of "repair" has caused a new hardware incompatibility because of their unique hardware and system configuration.

  The legislation does not define a specific mechanism to deliver a repair or a replacement. We agree with this approach. But if the Bill ultimately does include "repair or replacement" as a remedy for providers of dynamic, service-based content (we believe it should not), we strongly recommend that the Explanatory Note and implementing guidance recognise that the repair or replacement mechanisms may simply require that software developers build and release patches for significant known issues in good faith. In addition, it should be noted that many "repairs" (i.e., patches) are costly and difficult to develop, unlike for physical goods, and teams of software engineers sometimes need several months to develop an effective patch. The proposed legislation should reflect these complexities better than it does at present.

- **The requirement that compensation be due for damage to other digital content or devices caused by faulty digital content (Clause 48) will inhibit innovation**. While developers test software, and software updates, against well-known system configurations, it is impossible to rule out system incompatibilities that result in damage to other digital content or devices. Additionally, some types of update – such as security updates – must be developed and distributed quickly, to inoculate more users more quickly against fast-growing security threats. In those cases, a small number of users may experience new difficulties as a result of the update, but a greater number are saved from being infected with a virus or otherwise harmed.

  Clause 48 will compel software developers to extensively test updates well beyond what is reasonable based on a risk-benefit analysis that weighs the potential harm against the

possible security advantages. As a result of this more extensive – and lengthier – testing, users will be put at risk. There may also be a conflict between clause 48 and the "right to repair", as software developers choose between taking on liabilities by rolling out a patch that creates issues for some customers or breaching their obligation to repair.

We recommend that clause 48 be re-worked, so that it does not prevent companies from innovating with new updates, and so that it does not delay the roll-out of security patches in particular.

- **The requirement that liability that cannot be excluded or restricted (Clause 49) will slow down the release of new products, would reduce consumer choice and undermine the richness and heterogeneity of the user experience.**

  It appears that this prohibition would extend to all liabilities, not only those specified in proposed sections 45 and 46. Therefore this provision would have the unintended consequence of rendering software manufacturers liable for damage caused to users' devices. In this situation, software developers would have to predict or anticipate the behaviour of their application in the software ecosystem. Specific applications can behave erratically as a result of their interaction with another product or due to setting modifications by the end-user, and this is impossible for software providers to predict Even if each line of code is wholly error free, no software vendor can guarantee that its products will operate faultlessly when interacting and interoperating with other vendor's technologies.

  Changes to the regime for software and digital content services will naturally encourage vendors to offer packages and solutions that are vertically integrated and that do not allow interoperability because by doing so they would be in a better position to manage their risk of liability. This would reduce consumer choice, undermine the richness and heterogeneity of the user experience, and run counter to industry's drive for more product interoperability.
  .

A further key point, made in our previous consultation submission to the Secretary of State for Business, Innovation, and Skills, is that the draft CR Bill's rules go further than, and are not compatible with, the European Consumer Rights Directive. This means that the UK will effectively create a two-tiered system of consumer rights in Europe for digital content, creating confusion for customers, extra costs for businesses, and frustrating the intent of the Consumer Rights Directive, which was to create a single digital market across Europe.

BSA and its members are not against the introduction of robust consumer rights for digital content. Stronger, clearer consumer rights will strengthen consumer trust in our industry, opening the way for more growth in the sector. However, the current draft CR Bill fails to take into account our industry's complexities, and instead attempts to shoehorn pre-digital concepts from sale of goods laws into a new and rapidly developing sector. BSA would ask that the UK Government consider carefully how each of the draft CR Bill's "digital rights" would work in practice. In too many cases in the current draft, the result would be consumer confusion and business uncertainty.

Therefore, BSA encourages the BIS Committee to re-work Chapter 3 of the CR Bill, to ensure that the consumer rights set out for digital content are well adapted to the industry to which they will be applied.

* * *

For further information, please contact Thomas Boué, Director, Government Relations EMEA, thomasb@bsa.org or Tel: +32.2.274.1315