COUNTRY: **UNITED STATES**

SCORE: 79.73 | RANK: 3/24

The United States has comprehensive and up-to-date laws in place for e-commerce, electronic signatures, and cybercrime. The US has signed and implemented the Convention on Cybercrime and plays a leading role in the investigation of global cybercrime.

Although no general privacy laws are in place, the US still had a busy year in 2012 in relation to privacy protection. A new Consumer Privacy Bill of Rights was published, and work has begun on its potential implementation through enforceable codes of conduct. The key regulator, the Federal Trade Commission, also had a very active year enforcing existing sectoral rules.

The US approach to interoperability improved in 2012 with new standards developed for cloud services by the National Institute of Standards and Technology.

Intellectual property protection in the United States remains mixed. The US has signed all of the relevant international agreements, and a strong enforcement culture is in place. However, multiple conflicting court decisions leave considerable legal uncertainty about what constitutes an online copyright breach.

The United States is an active participant in international standards development processes and an advocate of free trade and harmonization. Some very limited domestic preferences remain in place for government procurement opportunities.

The United States has high levels of Internet use, but access to fast broadband remains patchy. The US has the 4th highest number of FttX connections and it has (by a considerable margin) the largest number of active mobile broadband connections.

Overall, the United States improved its ranking by one spot to 3rd in the 2013 Scorecard through a combination of positive policy developments and improved ICT infrastructure.

Q	UNITED STATES	RESPONSE	EXPLANATORY TEXT
	DATA PRIVACY		
1.	Are there laws or regulations governing the collection, use, or other processing of personal information?	◑	There is no single privacy law in the US. A range of specific, sectoral laws impose privacy obligations in specific circumstances. There are numerous gaps and overlaps in coverage. Several attempts have been made, without success, to introduce more comprehensive privacy legislation. In February 2012 the White House released a new framework for privacy protection. "Consumer Data Privacy in a Networked World: A Framework for Protecting and Promoting Innovation in the Global Digital Economy" <www.whitehouse.gov/sites/default/files/privacy-final.pdf> introduces the concept of a Consumer Privacy Bill of Rights, a set of guiding principles that can be incorporated into enforceable codes of conduct. To date, these principles have not been implemented in practice, but work is progressing on developing codes and other regulatory tools to implement them.
2.	What is the scope and coverage of privacy law?	Sectoral	Current sectoral privacy laws include: • The Federal Trade Commission Act — prohibits unfair or deceptive practices and this requirement has been applied to company privacy policies in several prominent cases; • The Electronic Communications Privacy Act — protects consumers against interception of their electronic communication (with numerous exceptions); • The Health Insurance Portability and Accountability Act (HIPAA) — contains privacy rules applying to certain categories of health and medical research data; and • The Fair Credit Reporting Act — includes privacy rules for credit reporting and consumer reports.

Q UNITED STATES	RESPONSE	EXPLANATORY TEXT
3. Is the privacy law compatible with the Privacy Principles in the EU Data Protection Directive?	◑	The US approach to privacy law is quite different from the EU approach. As there are significant gaps in US coverage, the US approach is not compatible with the EU Directive for all sectors or all organizations. However, individual organizations can "opt-in" to a voluntary, self-certification scheme — the US Safe Harbor <export.gov/safeharbor> — that is recognized as adequate by the EU. This scheme excludes some large business categories such as financial services and telecommunications. Enforcement and compliance within the scheme is patchy, although recent enforcement actions by US regulators have included direct action for breaches of the Safe Harbor framework. Only a small fraction of US companies maintain up-to-date membership of the scheme. Privacy protection in other sectors, especially the health sector, is governed by strong sectoral laws that provide a level of protection similar to that available in Europe.
4. Is the privacy law compatible with the Privacy Principles in the APEC Privacy Framework?	◑	The patchwork of US privacy laws is partially compatible with the APEC privacy framework. However, for the many companies that are not covered by sectoral laws and that have not opted in to self-regulatory schemes, no privacy protection is available.
5. Is an independent private right of action available for breaches of data privacy?	Available	There is no specific right to privacy in the US Constitution. However, various Supreme Court cases have found that a limited constitutional right of privacy exists, based on a combination of provisions in the Bill of Rights and subsequent amendments. See for example: Katz v. US, 386 US 954 (1967) <laws.findlaw.com/US/386/954.html>. Individual actions and class actions are very common, usually based on a mix of constitutional rights and consumer laws.
6. Is there an effective agency (or regulator) tasked with the enforcement of privacy laws?	Sectoral regulator	A number of organizations have a limited privacy oversight role, including the Federal Trade Commission (FTC), the Department of Commerce (for the US Safe Harbor members) and some specific federal and state sectoral regulators. No single organization has an over-arching privacy regulatory role. In 2012, US regulators took a range of significant enforcement action in relation to privacy breaches. These high-profile cases and campaigns help to strengthen overall privacy protection in the United States.
7. What is the nature of the privacy regulator?	Other government official	A wide variety of regulators are in place; most are appointed government officials.
8. Are data controllers free from registration requirements?	✔	There are no general registration requirements in place in the US.
9. Are cross-border transfers free from registration requirements?	◑	There are no restrictions or registration requirements in the US relating to cross-border transfers of data from the US to other countries. However, organizations that wish to be members of the Safe Harbor must register with the Department of Commerce, including an annual renewal requirement and a registration fee.
10. Is there a breach notification law?	✔	There are numerous — but inconsistent — state data breach notification laws in place in the US. Typically these require notification both to an appropriate regulator (e.g., the relevant state attorney general) and to the affected consumers. A federal data breach notification law is under consideration.
SECURITY		
1. Is there a law or regulation that gives electronic signatures clear legal weight?	✔	The Uniform Electronic Transactions Act 1999 establishes the legal equivalence of electronic records and signatures with paper writings and manually signed signatures, removing barriers to electronic commerce. The Electronic Signatures in Global and National Commerce Act 2000 (the ESIGN Act) provides a more detailed legal framework for recognizing electronic signatures
2. Are ISPs and content service providers free from mandatory filtering or censoring?	✔	The courts have regularly upheld the First Amendment right to free speech in the US Constitution and struck down laws intended to regulate access to Internet content. No current filtering or censorship is in place in the US.
3. Are there laws or enforceable codes containing general security requirements for digital data hosting and cloud service providers?	Limited coverage in legislation	There is no general security requirement in US law. However, there are numerous sectoral security requirements, especially in relation to financial services and health data. Some of these requirements can be very specific, including requirements to encrypt data and take steps to identify identity fraud. One state (California) imposes stronger security requirements (including encryption) for most databases containing personal information.

Q UNITED STATES	RESPONSE	EXPLANATORY TEXT
4. Are there laws or enforceable codes containing specific security audit requirements for digital data hosting and cloud service providers?	Limited coverage in legislation	There are no specific enforceable security audit requirements in place in the US. In the absence of privacy laws, most security requirements stem from consumer law. For example, a company that hosts data and claims to hold the data securely may face consequences for misleading consumers about that claim. The FTC occasionally takes action against online businesses that have poor security audit practices. Private actions and class actions for security breaches are also common in the US, and this litigation tends to act as a default security audit requirement. Additional security standards are in place in sectoral laws and guidelines. For example, HIPAA of 1996 (P.L.104-191) security requirements in the health sector, the Payment Card Industry Data Security Standard (PCI DSS) in the payments industry sector, and security audit requirements in relevant credit reporting legislation
5. Are there security laws and regulations requiring specific certifications for technology products?	Comprehensive requirements (including common criteria)	The United States is the world's most active user of security certifications for technology products and implements the international Common Criteria program in the majority of domestic IT procurement rules. The US is a Certificate Producer Member (the highest level of membership) of the Common Criteria Recognition Arrangement <www.commoncriteriaportal.org>.
CYBERCRIME		
1. Are cybercrime laws in place?	✔	There are several relevant statutes in the US. The key cybercrime provisions are contained in the Federal Computer Fraud and Abuse Act (CFAA), 18 USC 1030. Other provisions appear in the PATRIOT Act and other minor statutes.
2. Are cybercrime laws consistent with the Budapest Convention on Cybercrime?	✔	US law is compatible with the Convention on Cybercrime. The US ratified the Convention in 2006.
3. What access do law enforcement authorities have to encrypted data held or transmitted by data hosting providers, carriers, or other service providers?	Not stated	The law on access to encrypted data is the subject of current court action — US v. Fricosu, 2011. The position remains unclear while this case is proceeding. The US Constitution's Fifth Amendment, which protects a citizen's right to remain silent in some circumstances, would appear to protect accused parties from having to reveal encrypted data. The application of this test to data held by third parties remains uncertain. In most cases, access with a warrant is probably sufficient. Progress in the current test case can be monitored at <www.eff.org/cases/us-v-fricosu>.
4. How does the law deal with extraterritorial offenses?	Limited coverage	The CFAA (18 USC 1030) has no specific extraterritorial provisions. However, the Uniting and Strengthening America by Providing Appropriate Tools required to Intercept and Obstruct Terrorism Act 2001 (the USA PATRIOT Act) includes provisions relating to a computer located outside the US that is used in a manner that affects interstate or foreign commerce or communication of the United States, for terrorism or fraud.
INTELLECTUAL PROPERTY RIGHTS		
1. Is the country a member of the TRIPS Agreement?	✔	The United States became a member of the TRIPS Agreement in 1995.
2. Have IP laws been enacted to implement TRIPS?	✔	The United States has implemented the TRIPS Agreement in its local copyright legislation.
3. Is the country party to the WIPO Copyright Treaty?	✔	The United States signed the WIPO Copyright Treaty in 1997 and ratified it in 1999. It entered into force in the United States in March 2002.
4. Have laws implementing the WIPO Copyright Treaty been enacted?	✔	The Digital Millennium Copyright Act implements the WIPO Copyright Treaty provisions in the US.
5. Are civil sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	◑	Section 106(3) of the Copyright Act would appear to include a "making available" right, in accordance with the US commitments under international copyright agreements. However, court interpretation of this section is inconsistent, with some courts arguing that further copying and distribution must occur rather then merely making the copyright material available. The leading case, involving multiple litigation over a number of years, is Capitol v. Thomas-Rasset (2008-2012, various citations). The latest decision in the case (September 2012, Court of Appeals, 8th Circuit) ruled that the high level of statutory damages imposed for wilful copyright infringement is constitutionally valid, as it is intended to serve a public interest purpose in discouraging illegal file sharing. However, the Court of Appeals failed to rule on the legality of "making available," finding that the case could be resolved on other grounds.

Q UNITED STATES	RESPONSE	EXPLANATORY TEXT
6. Are criminal sanctions available for unauthorized making available (posting) of copyright holders' works on the Internet?	◑	On paper, criminal sanctions are available for any wilful infringement of copyright in the US. However, due to the uncertainty that has arisen in "making available" decisions resulting from civil proceedings, there has been no action in the US to pursue criminal sanctions for "making available." Criminal sanctions for other infringements have generally been used sparingly with a mix of low fines and probation. However, the severity of sanctions has increased steadily in recent years.
7. Are there laws governing ISP liability for content that infringes copyright?	✔	The Online Copyright Infringement Liability Limitation Act (OCILLA) creates a safe harbor for ISPs by shielding them for certain acts of copyright infringement, as long as they were not aware of the infringement and they respond promptly to take-down requests. These provisions now form Section 512 of the Digital Millennium Copyright Act (DMCA), and notices are typically referred to as DMCA Takedown Notices. Where the ISP safe harbor conditions are not met, US common law on copyright applies. In these cases there is considerable uncertainty about the extent of ISP liability for breaches outside their direct control.
8. Is there a basis for ISPs to be held liable for content that infringes copyright found on their sites or systems?	✔	ISPs may be held liable for infringing content that they were made aware of if they do not meet the safe harbor conditions in the DMCA.
9. What sanctions are available for ISP liability for copyright infringing content found on their site or system?	Civil and criminal	A full range of civil penalties is available. Criminal sanctions are more limited and do not apply to all copyright infringements.
10. Must ISPs take down content that infringes copyright, upon notification by the right holder?	✔	The use of DMCA take-down notices is widespread in the US. Subject to certain limited exceptions, the notices are usually enforceable.
11. Are ISPs required to inform subscribers upon receiving a notification that the subscriber is using the ISP's service to distribute content that infringes copyright?	◑	US ISPs voluntarily pass on copyright breach notices and alerts to subscribers. This does not appear to be an enforceable requirement of any law; it has simply become common business practice.
12. Is there clear legal protection against misappropriation of cloud computing services, including effective enforcement?	Comprehensive protection	The US provides useful layers of protection through its cybercrime laws and copyright laws. There is some uncertainty about the application of copyright laws to online posting, and there are gaps in privacy law, but overall the level of protection available for cloud computing services is adequate.
SUPPORT FOR INDUSTRY-LED STANDARDS & INTERNATIONAL HARMONIZATION OF RULES		
1. Are there laws, regulations or policies that establish a standards-setting framework for interoperability and portability of data?	✔	There is no specific legislation on national standards in the US, but the development of standards is guided by a policy document, the United States Standards Strategy www.ansi.org/standards_activities/nss/usss.aspx, that is regularly updated. The National Institute of Standards and Technology (NIST) <www.nist.gov> is the organization that has carriage of cloud computing standards. In 2012 NIST issued formal guidelines for managing security and privacy issues in cloud computing: Guidelines on Security and Privacy in Public Cloud Computing (NIST Special Publication 800-144).
2. Is there a regulatory body responsible for standards development for the country?	✔	The American National Standards Institute (ANSI) <www.ansi.org> is a non-profit organization that represents the US in international standards development processes. ANSI itself does not develop standards; it oversees the development and use of standards by accrediting the procedures of standards developing organizations. NIST is the relevant standards-setting body for the digital economy and cloud computing.
3. Are e-commerce laws in place?	✔	The Uniform Electronic Transactions Act (UETA) has helped to implement consistent e-commerce laws in 47 US jurisdictions.
4. What international instruments are the e-commerce laws based on?	Other	US legislation, including separate digital signature and e-commerce legislation, is unique and is not based on any international instrument. However, the core rules are similar to the UNCITRAL Model Law on E-Commerce.
5. Is the downloading of applications or digital data from foreign cloud service providers free from tariff or other trade barriers?	✔	There are no relevant tariffs in the United States. However, US Internet gambling laws have been interpreted as non-tariff trade barriers in several WTO and EU court rulings. These restrictions are unlikely to have a significant impact on the digital economy or cloud computing.
6. Are international standards favored over domestic standards?	✔	Most relevant standards in the US have been developed through international cooperation, and US standards either reflect international standards or are themselves adopted as international standards.

Q UNITED STATES	RESPONSE	EXPLANATORY TEXT
7. Does the government participate in international standards-setting process?	✔	Both ANSI and NIST participate in relevant international standards-setting processes.
PROMOTING FREE TRADE		
1. Are any laws or policies in place that implement technology neutrality in government?	✔	The US government has a formal policy in place: Making Technology Neutral IT Procurement Decisions 2011 <www.cio.gov/documents/Technology-Neutrality.pdf>.
2. Are cloud computing services able to operate free from laws or policies that mandate the use of certain products (including, but not limited to, types of software), services, standards, or technologies?	✔	There are no relevant mandatory requirements in the United States.
3. Are cloud computing services able to operate free from laws or policies that establish preferences for certain products (including, but not limited to, types of software), services, standards, or technologies?	✔	There are no relevant preferences in place in the United States.
4. Are cloud computing services able to operate free from laws that discriminate based on the nationality of the vendor, developer, or service provider?	◑	The US does impose some domestic preferences in legislation. The Buy American Act (BAA) 1933 (and regularly updated) contains broad domestic preferences for US procurement. It mainly covers the construction sector, but many other products are caught by the provisions. In 2009, BAA was amended by the American Recovery and Reinvestment Act (ARRA), which included a prohibition on ARRA funds being used in projects that did not involve US goods and services. The Buy America provisions rarely apply to the ICT sector. Since 2004 the Buy America Act has included an exemption for the purchase of any "commercial information technology product." The exact test used in the exemption is quite complex, and not all IT services will be exempt. There has not yet been a relevant test case on cloud computing.
ICT READINESS, BROADBAND DEPLOYMENT		
1. Is there a national broadband plan?	• By 2020, at least 100 million homes to have affordable access to download speeds of 100 Mbps and upload speeds of 50 Mbps • By 2020, every household to have access to download speeds of 4 Mbps and upload speeds of 1 Mbps	In 2010 the United States Federal Communications Commission unveiled the National Broadband Plan, "Connecting America" <www.broadband.gov>. The National Broadband Plan sets a number of goals: • By 2020 at least 100 million households to have download speeds of 100 Mbps and upload speeds of 50 Mbps; • By 2020, every community should have affordable access of at least 1 Gbps to anchor institutions (schools, hospitals, and government buildings). Not all parts of the plan have been adopted or fully funded, however significant parts of the plan have been implemented, including the rollout of the Connect America Fund in 2012, which addresses broadband coverage in rural areas.
2. Are there laws or policies that regulate the establishment of different service levels for data transmission based on the nature of data transmitted?	Regulation under consideration by government and extensive public debate	Net neutrality is a high-profile and controversial issue in the United States. There is no specific net neutrality legislation in place at a federal level, although there have been numerous failed attempts to pass legislation. The FCC approved the Open Internet Order on December 21m 2010 <transition.fcc.gov/Daily_Releases/Daily_Business/2010/db1223/FCC-10-201A1.pdf>. It establishes basic principles of transparency and non-discrimination, while allowing some prioritization of traffic for management purposes. However, the FCC's order is non-binding as the result of Comcast v. FCC, 600 F.3d 642, 2010 (United States Court of Appeals for DC Circuit), which decided that the FCC did not have sufficient jurisdiction to enforce its guidance on net neutrality in the absence of specific legislation.

Q UNITED STATES	RESPONSE	EXPLANATORY TEXT
3. Base Indicators		
3.1. Population (2011)	313,085,380	In 2011, the population of the United States increased by 0.7%. [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2012) <www.itu.int/ITU-D/ict/publications/world/world.html>]
3.2. Urban Population (%) (2011)	82%	[United Nations, Department of Economic and Social Affairs, Population Division (2012). World Urbanization Prospects: The 2011 Revision, <esa.un.org/unup/CD-ROM/Urban-Rural-Population.htm>]
3.3. Number of Households (2011)	119,300,000	In 2011, the number of households in the US increased by 1.6%. [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2012) <www.itu.int/ITU-D/ict/publications/world/world.html>]
3.4. Population Density (people per square km) (2010)	34	[World Bank, Data Catalog, Indicators, Population Density (2012) <data.worldbank.org/indicator/EN.POP.DNST>]
3.5. Per Capita GDP (US$ 2011)	$48,442	In 2011, the per capita GDP for the US increased by 1.7% to US$48,442. [World Bank, Data Catalog, Indicators: GDP per capita, current US$ (2012) <data.worldbank.org/indicator/NY.GDP.PCAP.CD> and GDP growth, annual % (2012) <data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG>]
3.6. Public Cloud Services Market Value (2011) (Billions of US$)	50.50	Gartner has calculated the value of the public cloud services market in the US in 2011 to be US$50.50 billion. This is a 19% increase from 2010 and ranks the US 1 (out of 20 countries) in the forecast. Gartner has projected the five-year compound annual growth rate (CAGR) to 2016 to be 19% and this ranks the US 11 (out of 20 countries) for growth in the value of the market for public cloud services to 2016. [Gartner, Forecast Overview: Public Cloud Services, Worldwide, 2011-2016 (August 2012 Update) <www.gartner.com/id=2126916>]
3.7. Personal Computers (% of households) (2011)	77%	In 2011, 77.2% of households in the US had personal computers. This is a 2.2% increase since 2010 and ranks the US 30 out of 182 countries surveyed. The growth from 2010 is below the five-year CAGR from 2006 to 2011 of 2.6%. [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2012) <www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx>] Note: In some jurisdictions this is an estimate and subsequent editions of the ITU ICT Indicators Database may update this indicator for prior years.
4. ICT and Network Readiness Indicators		
4.1. ITU ICT Development Index (IDI) (2011) (Score is out of 10)	7.48	The US ITU ICT Development Index (IDI) for 2011 is 7.48 (out of 10), resulting in a rank of 15 (out of 161 economies). The 2011 IDI for the US has increased by 5.2%, and the IDI ranking has improved by one place from a rank of 16 since 2010. [International Telecommunication Union (ITU), Measuring the Information Society (2012) <www.itu.int/ITU-D/ict/publications/idi/2012>] Note: In some jurisdictions this is an estimate and subsequent editions of the ITU ICT Indicators Database may adjust this indicator, both for 2011 and prior years.
4.2. World Economic Forum Networked Readiness Index (NRI) (2012) (Score is out of 7)	5.43	The US has a Networked Readiness Index (NRI) score of 5.43 (out of 7), resulting in a rank of 5 (out of 142 economies) and a rank of 5 (out of 47) in the high income grouping of economies. The 2012 NRI for the US has increased by 1.8% and the ranking has remained the same since 2011. [World Economic Forum, Global Information Technology Report (2012) <www.networkedreadiness.com/gitr>]
4.3. International Connectivity Score (2011) (Score is out of 10)	7.82	The US has a Connectivity Score of 7.82 (out of 10), resulting in a rank of 1 (out of 25) in the innovation-driven grouping of countries/economies. [Nokia Siemens, Connectivity Scorecard (2011) <www.connectivityscorecard.org>]
4.4. IT Industry Competitiveness Index (2011) (Score is out of 100)	80.50	The US has an IT Industry Competitiveness Index Score of 80.5 (out of 100), resulting in a rank of 1 (out of 66 countries/economies included in the index). The 2011 index score is a 0% increase on the 2009 score. The US has kept the same ranking since 2009. [Business Software Alliance (BSA) / Economist Intelligence Unit (EIU), IT Industry Competitiveness Index (2011) <globalindex11.bsa.org>]

Q UNITED STATES	RESPONSE	EXPLANATORY TEXT
5. Internet Users and International Bandwidth		
5.1. Internet Users (2011)	243,777,735	[calculated from 8.3.1. and 8.5.2.]
5.2. Internet Users as % of Population (2011)	78%	In 2011, 78% of the population in the US used the Internet, resulting in a ranking of 27 out of 199 countries surveyed. This is a 5.2% increase since 2010. The growth from 2010 is above the five-year CAGR from 2006 to 2011 of 2.5%. [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (December 2012) <www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx>] Note: There may be some variations as to how countries calculate this. Some countries base this upon all or part of the population, such as between 16 and 72 years of age. Note: In some jurisdictions this is an estimate and subsequent editions of the ITU ICT Indicators Database may adjust this indicator, both for 2011 and for prior years.
5.3. International Internet Bandwidth (bits per second per Internet user) (2011)	47,174	The US International Internet Bandwidth (per Internet user) has increased by 20% since 2010. [International Telecommunication Union (ITU), Measuring the Information Society (2012) <www.itu.int/ITU-D/ict/publications/idi/2012>]
5.4. International Internet Bandwidth (2011) (total gigabits per second [Gbps] per country)	11,500	The US has increased its International Internet Bandwidth by 28% since 2010 to 11,500 Gbps and is ranked 1 out of 188 countries surveyed. The growth from 2010 is below the five-year CAGR from 2006 to 2011 of 41.3%. [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2012) <www.itu.int/ITU-D/ict/publications/world/world.html>]
6. Fixed Broadband		
6.1. Fixed Broadband Subscriptions (2011)	85,630,000	The US has increased the number of fixed broadband subscribers by 3% since 2010, to 85,630,000, and is ranked 2 out of 182 countries surveyed. The growth from 2010 is below the five-year CAGR from 2006 to 2011 of 7.3%. [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2012) <www.itu.int/ITU-D/ict/publications/world/world.html>] Note: In some jurisdictions this is an estimate and subsequent editions of the ITU ICT Indicators Database may adjust this indicator, both for 2011 and prior years.
6.2. Fixed Broadband Subscriptions as % of Households (2011)	72%	[calculated from 8.3.3. and 8.6.1.] Note: This may be skewed by business usage in some countries (refer to OECD comments about this).
6.3. Fixed Broadband Subscriptions as % of Population (2011)	27%	The US has increased its fixed broadband subscriptions (as a share of the population) by 3% since 2010, which is below the five-year CAGR from 2006 to 2011 of 6.3%. This ranks the US 2 out of 187 countries surveyed. The OECD figures below present a breakdown on the type of fixed broadband connections in the US in 2011. The US is distinguished by having one of the highest proportion of cable connections in the OECD — and the subscription rate continues to increase for cable Internet subscriptions in 2011. The US has the highest total number of broadband subscriptions (by a considerable margin) in the OECD — 85.7 million. The US is following the trend (set largely by Japan and Korea) of declining DSL subscription rates and increasing fiber connections. In the OECD, the US was ranked 15 (out of 34) for fixed (wired) broadband subscribers as a percentage of population [OECD Broadband Subscribers (Dec 2011) <www.oecd.org/sti/ict/broadband>] – DSL: 10% (declined from 10.9% in 2010) – Cable: 15.5% (one of the higher proportions of cable connections in the OECD, surpassed only by Canada and the Netherlands) – Fiber/LAN: 1.9% – Other: 0.3% Total: 27.7% (85,723,155 subscriptions). The OECD average total for 2011 was 25.6%. The US fixed broadband growth for 2011 was 3.5% (ranked 25 out of 34 for growth), below the OECD average growth of 4.1%. Note: There may be minor variations in the ITU and OECD subscriber totals due to definition, timing or population baseline differences. [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (July 2011) <www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx>]

Q UNITED STATES	RESPONSE	EXPLANATORY TEXT
6.4. Fixed Broadband Subscriptions as % of Internet Users (2011)	35%	[calculated from 8.5.1 and 8.6.1]
7. Mobile Broadband		
7.1. Mobile Cellular Subscriptions (2011)	290,304,000	In 2011, the US increased the number of mobile cellular subscriptions by 1.8% and is ranked 3 out of 195 countries surveyed. The number of subscriptions account for 93% of the population. [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2012) <www.itu.int/ITU-D/ict/publications/world/world.html>] Note: This figure may be inflated due to multiple subscriptions per head of population but excludes dedicated mobile broadband devices (such as 3G data cards and tablets).
7.2. Active Mobile Broadband Subscriptions per 100 inhabitants (2011)	75%	The US has increased the number of active mobile broadband subscriptions (as a share of the population) by 37% since 2010. This ranks the US 10 out of 144 countries surveyed. The OECD figures below present a breakdown on the type of mobile broadband connections in the US. The US is distinguished by having the largest number of mobile broadband subscribers in the OECD — 235 million. For 2011, the US OECD rank has improved two places and was 2 (out of 34) for mobile wireless broadband subscribers as a percentage of population [OECD Broadband Subscribers (Dec 2011) <www.oecd.org/sti/ict/broadband>] – Satellite: 0.4% – Terrestrial fixed wireless: 0.2% – Standard mobile broadband subscription: 25.4% (down from 25.7% in 2010) – Dedicated mobile data subscriptions: 50.1% (up from 7.8%) Total: 76.1% (235,199,000 subscriptions). The OECD average total for 2011 was 54.3%. The US wireless broadband growth for 2011 was 42% (ranked 13 out of 34 for growth), above the OECD average growth of 30.5%. Note: The mobile broadband subscription types were first reported by OECD in 2010, and ITU data are beginning to have this granularity. Note: The OECD figures include mobile data subscriptions, which are not as consistently reported in the ITU indicators. [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2012) <www.itu.int/ITU-D/ict/publications/world/world.html>] Note: This refers to the sum of standard mobile broadband and dedicated mobile broadband subscriptions to the public Internet. It covers actual subscribers, not potential subscribers, even though the latter may have broadband-enabled handsets. Note: In some jurisdictions this is an estimate and subsequent editions of the ITU ICT Indicators Database may adjust this indicator, both for 2011 and prior years.
7.3. Number of Active Mobile Broadband Subscriptions (2011)	233,265,000	In 2011, the US increased the number of active mobile broadband subscriptions by 39% and is ranked 10 out of 145 countries surveyed. [International Telecommunication Union (ITU), World Telecommunication/ICT Indicators Database (Dec 2012) <www.itu.int/ITU-D/ict/publications/world/world.html>]