Moving Beyond Passwords: Consumer Attitudes on Online Authentication
A Study of US, UK and German Consumers

Sponsored by Nok Nok Labs, Inc.

Independently conducted by Ponemon Institute LLC

Publication Date: April 2013

Moving Beyond Passwords: Consumer Attitudes on Online Authentication
A Study of US, UK and German Consumers

Part 1. Introduction

A difficult security dilemma for companies is to have the appropriate level of identity and authentication practices in place without making it too difficult or inconvenient for consumers to shop, bank online, request services and do other favorite Internet activities. If their methods are lax, personal data is at risk. If too strict, revenues may be lost due to customer frustration when trying to get authenticated.

There are many other consequences of poor authentication. These include jeopardizing the security of passengers using public transportation and reducing efficiencies in providing products and services. Companies also risk losing the trust of their customers if authentication and identification methods fail.

Ponemon Institute and Nok Nok Labs decided to study this conundrum. We believe this the first study designed to probe consumers' perceptions about how organizations are confirming their identity and to learn what they would consider to be the ideal steps and technologies used to ensure their identity is protected.

We surveyed 1,924 consumers between the ages of 18 and 65+ in the United States, United Kingdom and Germany. In order to ensure a knowledgeable respondent, we used screening criteria. All respondents self-reported they spend a minimum of 10 hours each week using the Internet and social media and are engaged in such activities as online shopping, online banking, blogging and obtaining government services.

The study provides interesting insights into what consumers think about multi-use identity credential, use of biometrics for authentication purposes, organizations most trusted to manage ID credentials and the most important benefits of a single ID. The following findings reveal how consumers want to be authenticated and identified.

- **Many consumers favor a single identity credential for a variety of authentication purposes.** The majority of consumers would use a multi-purpose identity credential to verify who they are before providing secure access to data, systems and physical locations.

- **You can bank on it.** Banking institutions are considered the best for online validation and strong authentication and identity verification. Consumers in all countries believe banks would be the best to issue and manage a multi-purpose identity credential.

- **The benefits of a multi-purpose identity credential are convenience (US & UK consumers) and security (German consumers).** Identification and authentication when traveling, accessing the Internet and using social networks are the most popular reasons to have single ID.

- **There is no clear consensus on what devices would be preferred to manage their multi-purpose identity credential.** However, in the US more consumers would prefer their mobile devices for identification purposes. In the UK, it is RFID chips. German consumers seem to favor biometrics.

- **If consumers trust the organization, biometrics is acceptable to use for authentication.** Voice recognition and facial scan are the most acceptable types of biometric authentication. Least acceptable in the US and UK is an iris scan. In Germany, least favored are fingerprints.

- **Authentication is important when sharing devices with other users**. The majority of consumers believe it is important to have authentication that securely verifies their identity on devices that are shared with other (multiple) users.

Some other noteworthy findings include the following:

- Consumers seem to be complacent about the trustworthiness of the identity and authentication procedures of websites they access, with the exception of German consumers.

- Less stringent authentication and identification verification procedures do not seem to deter the majority of consumers from accessing websites, with the exception of German consumers.

- Industries and organizations considered by consumers in all three countries as most trustworthy to safely issue and manage a multi-purpose identity credential are: banking institutions, credit card and Internet payment providers, telephone, wireless or cable services companies, healthcare providers and postal and delivery services. Least trusted are educational institutions, Internet service providers and retailers.

- Most authentication failures happen because of forgotten passwords, usernames or a response to a fact-based question (such as a mother's maiden name).

- The majority of respondents believe it is acceptable for a trusted organization such as their bank, credit card companies, health care provider, telecom, email provider or governmental organization to use biometrics such as voice or fingerprints to verify their identity.

Part 2. Key Findings

The report is organized according to the following three topics:

- Experiences with identity and authentication online practices
- Perceptions about online authentication and identification
- Preferences for identity and authentication steps and technologies

1. Experiences with Identity and authentication online practices

Forgetting passwords, user names and answers to security questions is the most common reason for authentication failures. In the US, 63 percent of respondents say they were not authenticated because they could not remember a password, user name or response, as shown in Figure 1. Less than a majority of respondents say authentication failures occur because of glitches or inaccuracies within website systems or identity verification procedures.

Figure 1. Why authentication and identification fails
Strongly agree and agree response combined

US   UK   Germany
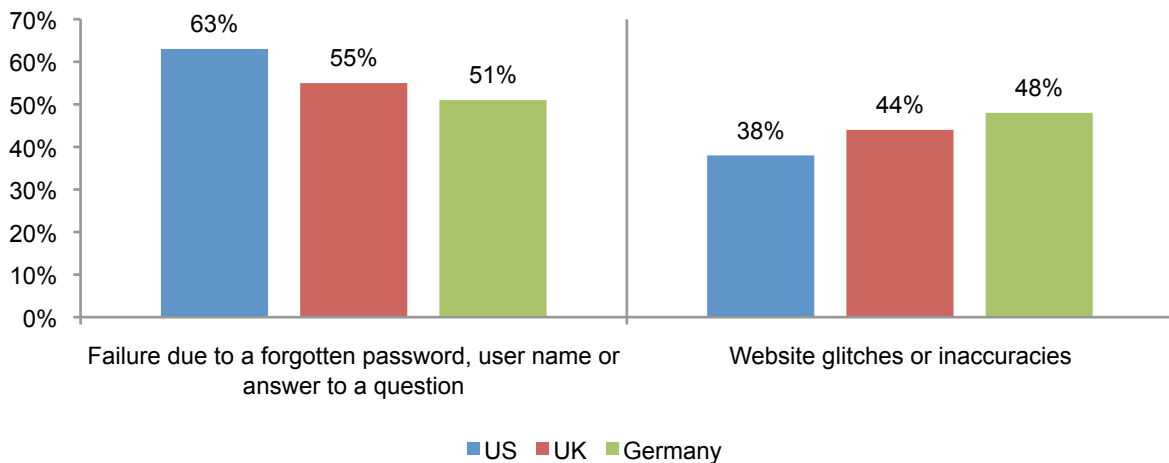
According to Figure 2, the most common experiences related to authentication failures are: forgetting a password because it was too long or complex, being locked out of an Internet site, and having to wait a long time to have username or password reset. German consumers have fewer authentication failures than those in the US and UK.

Figure 2. Consequences of authentication failure most often experienced
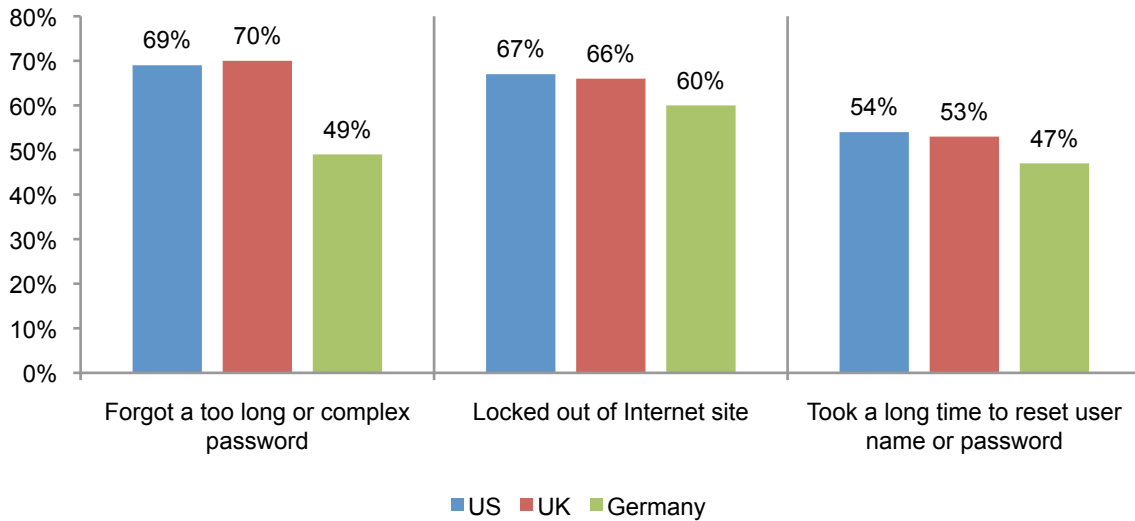Respondents who say it happened to them one or more times over the past 2 years

Figure 3 shows the consequences of authentication failures rarely experienced by consumers. These are: identity fraud, misuse of private information in a social media site (wall), could not complete a loan or mortgage transaction, as shown in Figure 3. Although it represents a low occurrence, 11 percent of German consumers did say an imposter misused their private information from their social media site, which is higher than for consumers in other countries.

**Figure 3. Consequences of authentication failures rarely experienced**
Respondents who say it happened to them one or more times over the past 2 years
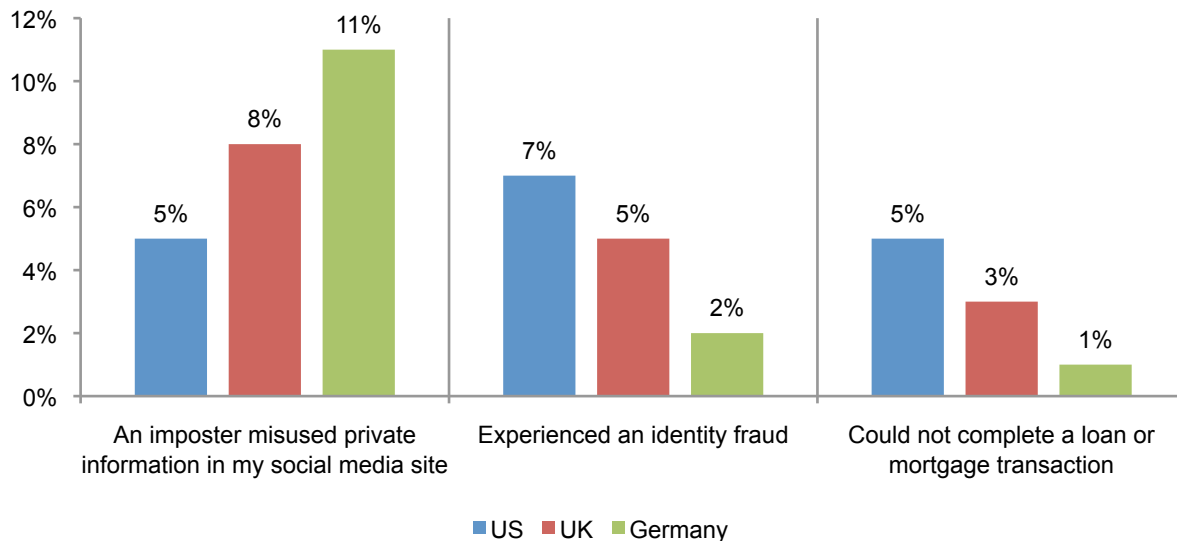
Failure to complete a transaction happens frequently. The majority of consumers in the UK and Germany say they were not able to perform an online transaction such as buying a product or obtaining a service because of an authentication failure on the website and found this experience frustrating, according to Figure 4. Less than half of US consumers (46 percent) failed to complete a transaction due to authentication failures.

As is understandable, the level of frustration is high for consumers in all countries. Seventy-five percent of US consumers say the situation is very frustrating or frustrating and 71 percent in both the UK and Germany agree.

Figure 4. Frequency of prohibited online transactions due to authentication failures


US   UK   Germany
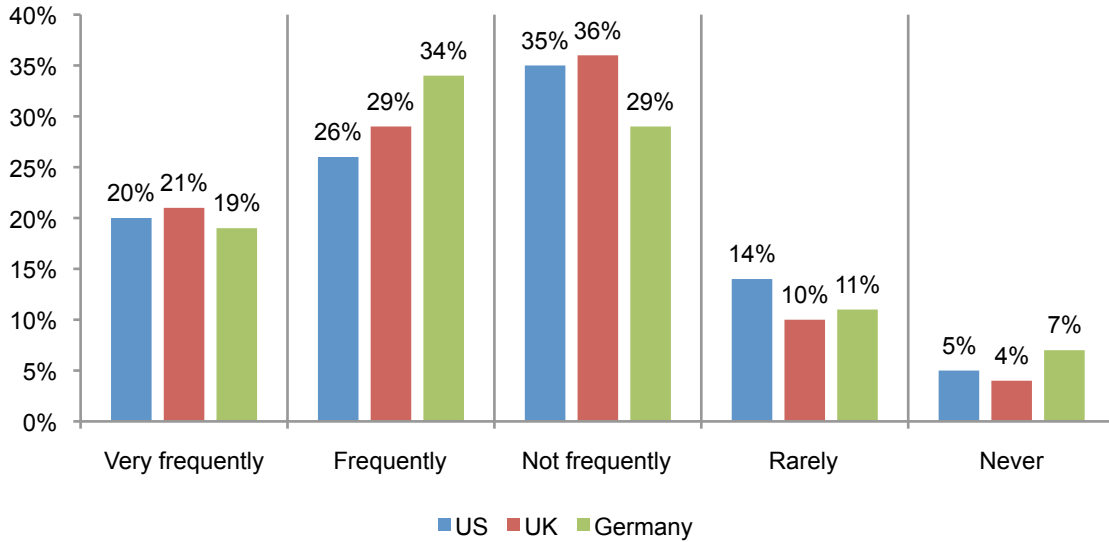
2. Perceptions about online authentication and identification

Some consumers' trust in a website's security may be dependent on the difficulty of authentication and identification practices. In the US and UK less than half of respondents believe that trust is dependent upon the use of more than passwords for authentication purposes. More German consumers (65 percent) do not trust systems or websites that only rely on passwords and user names (Figure 5).

There is some concern if consumers are not forced to regularly change passwords. Thirty-eight percent of US consumers and 37 percent of UK consumers say that this would diminish their trust. A higher percentage (46 percent) of German consumers are less likely to have trust in systems or websites if they don't require password changes on regular intervals.

Figure 5. The affect of weak password authentication and identification on consumer trust
Strongly agree and agree response combined

US   UK   Germany
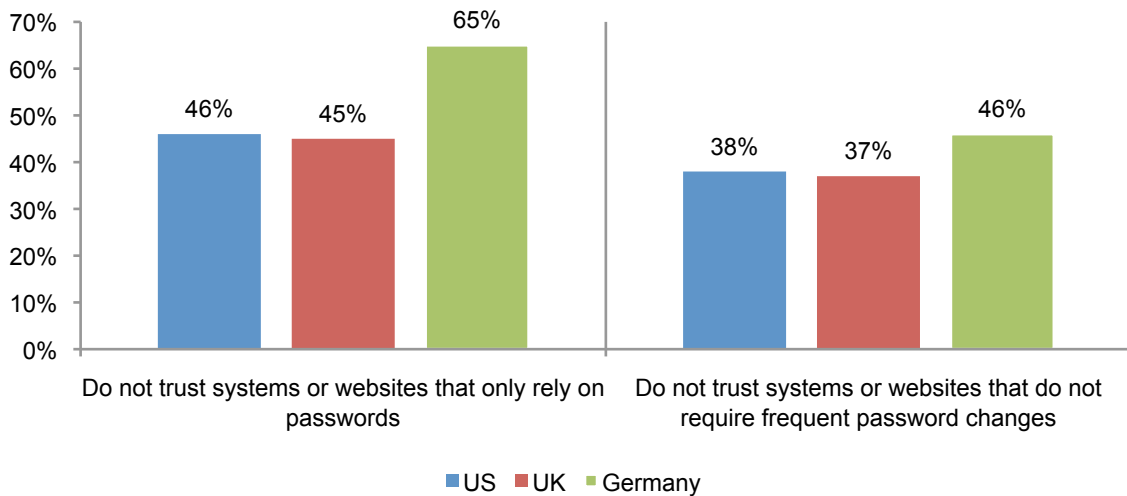
More than half of German consumers surveyed do not trust websites with inadequate authentication and identity verification procedures, as shown in Figure 6. Only 35 percent of U.S. consumers and 39 percent of UK consumers would avoid such websites. Further, identity and authentication procedures that appear too easy do not affect trust in systems or websites, with the exception of German consumers. Less than half of U.S. and UK consumers would avoid systems and websites with procedures that seem too easy.

Figure 6. Weak authentication and identity verification affect consumer trust
Strongly agree and agree response combined
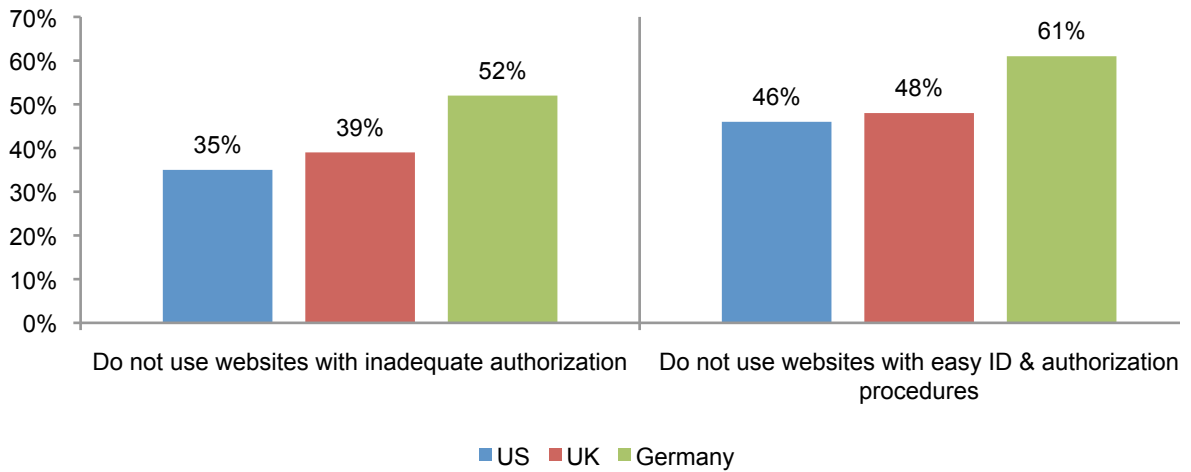
Certain organizations are considered the best at online validation. Most consumers in all countries expect certain organizations to have stronger authentication and identity verification. However, consumers in all three countries have similar perceptions about organizations that do the best job for all **online validations**.

As shown in Figure 7, the top five are: banking institutions, credit card and Internet payment providers, social media, retailers and Internet service providers. The complete list of organizations and response frequency is shown in the appendix to this report.

Figure 7. Organizations consumers believe do the best online validation
Three choices permitted
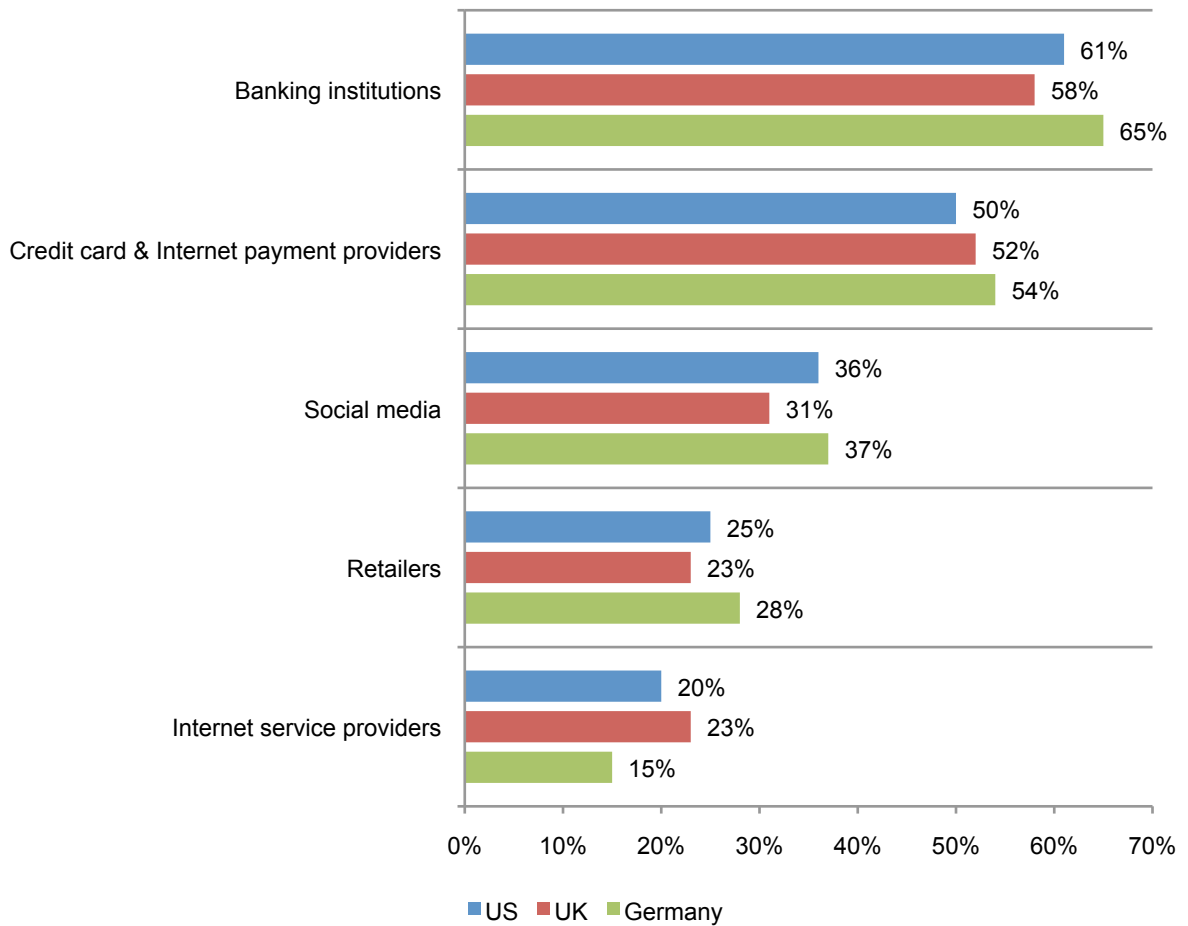
According to Figure 8, consumers in all three countries have exactly the same perception about organizations that do the best job for **physical validation**. The top five considered to do the best job with physical validation are: airlines, banking institutions, healthcare providers and federal government organizations. The complete list of organizations and response frequency is shown in the appendix to this report.

Figure 8. Organizations consumers believe do the best physical validation
Three choices permitted
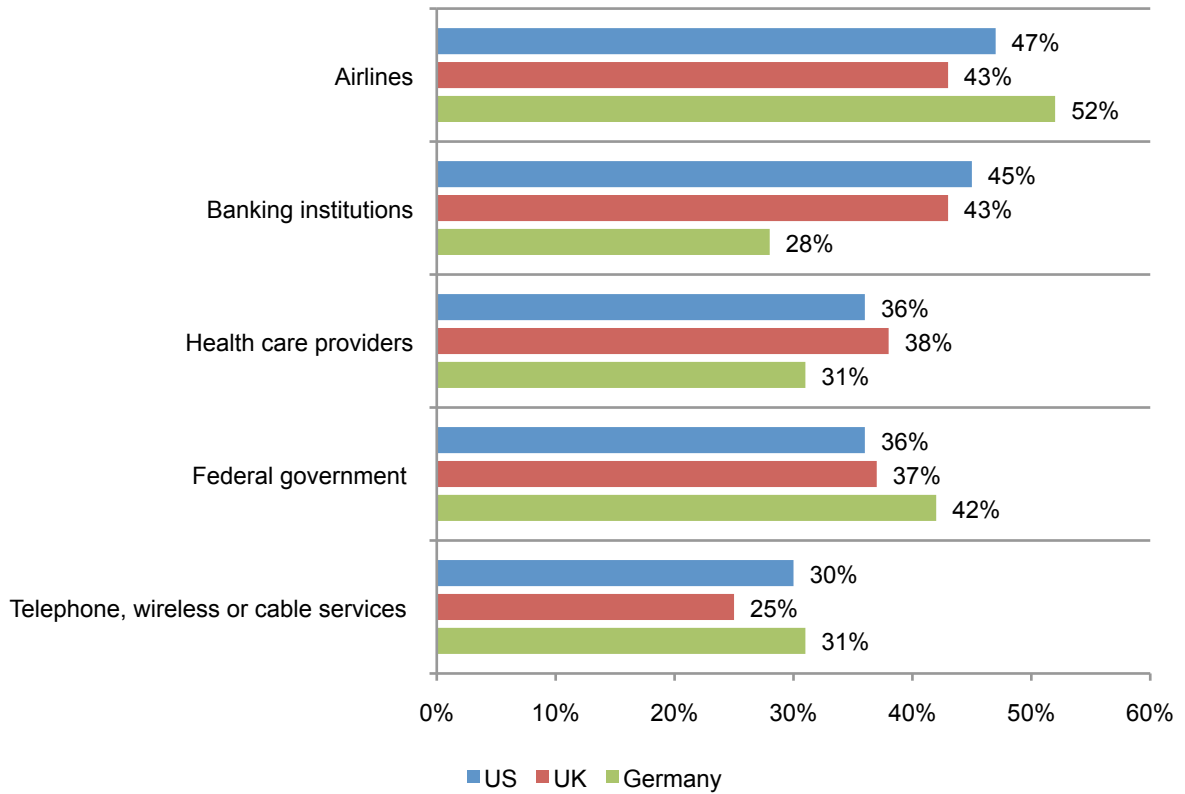
Figure 9 shows the top 10 organizations that consumers believe have the strongest methods for authentication and identity verification. Again banking institutions are consumers first choice followed by law enforcement. Expectations are lower for federal government and utilities. The complete list and frequency of response is shown in the appendix of this report.

Figure 9. Organizations with very strong authentication & identity verification methods
More than one response permitted
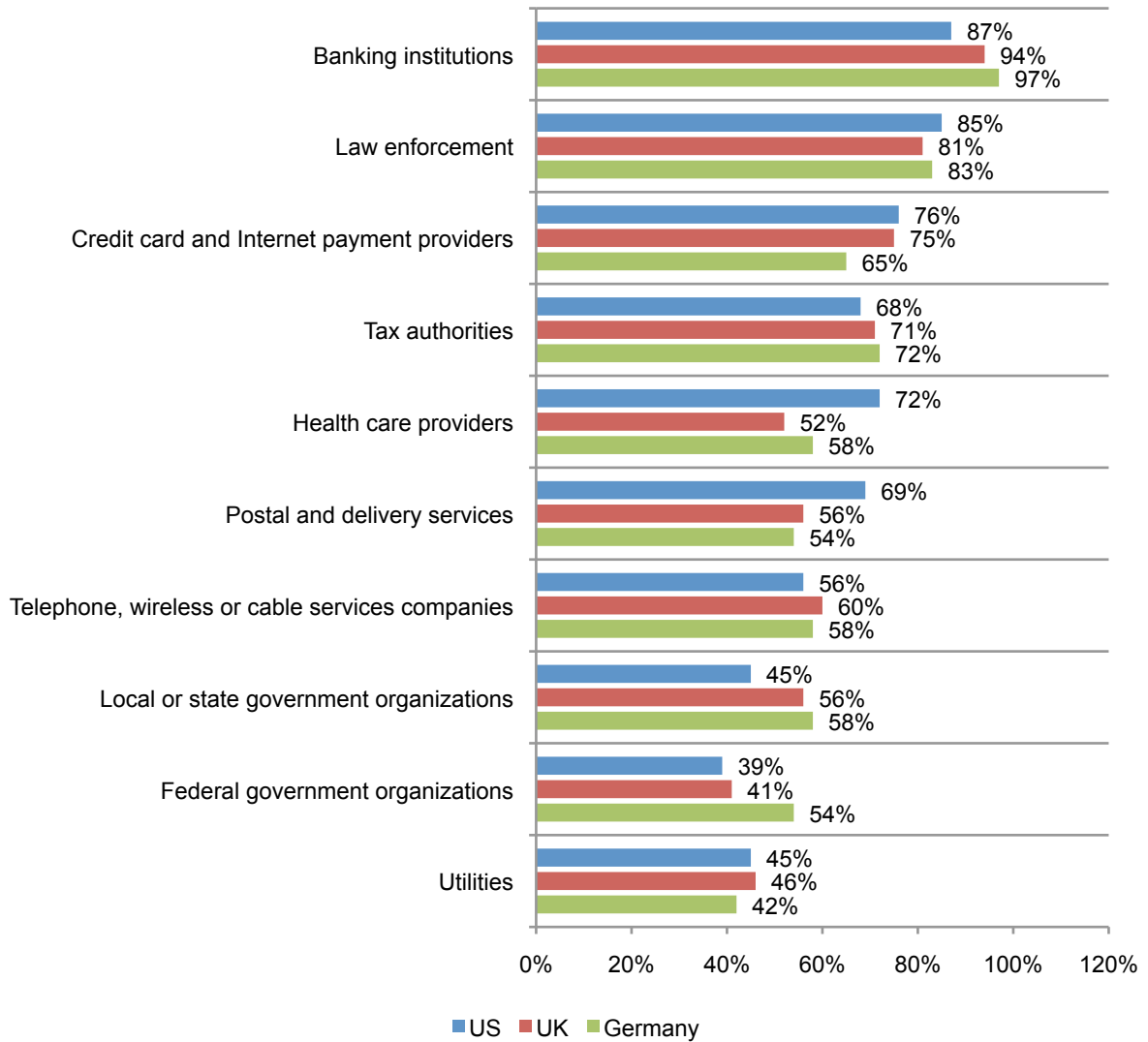
3. Preferences for identity and authentication steps and technologies

Verification without disclosing personal information is preferred. Consumers would prefer authentication procedures that verify their identity without having to share personal information such as name, address and email as shown in Figure 10. German consumers are most opposed to sharing personal information.

**Figure 10. Verification without requiring personal information preferred**
Strongly agree and agree response combined
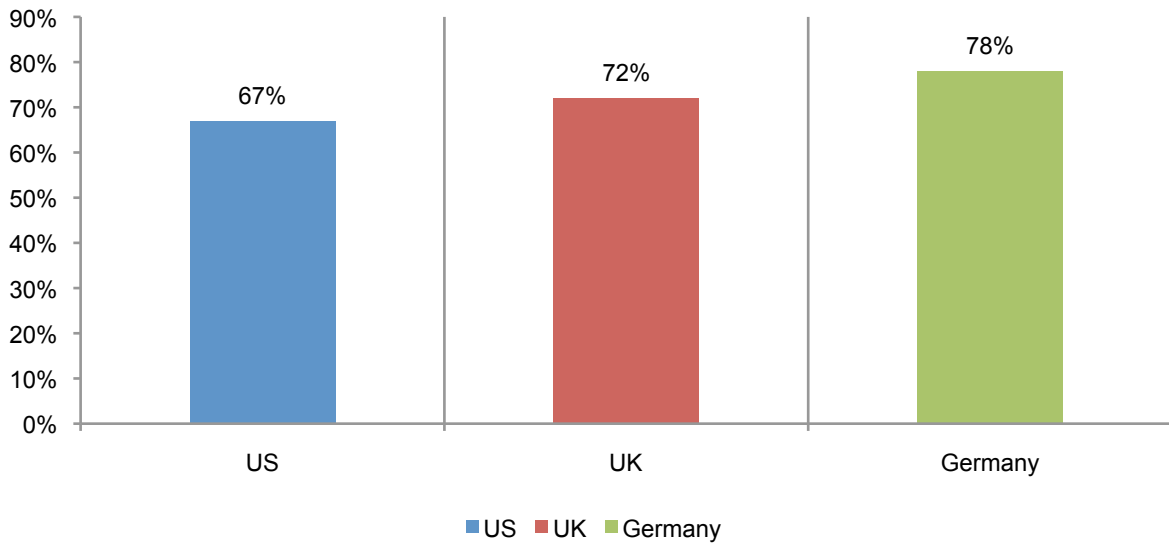
Certain information is acceptable to share with business and government. According to Figure 11, consumers in all three countries would be willing to share the following with a **business** organization: name, unique account number, email address and password or PIN.

Figure 11. Information consumers would share with a business organization
More than one response permitted
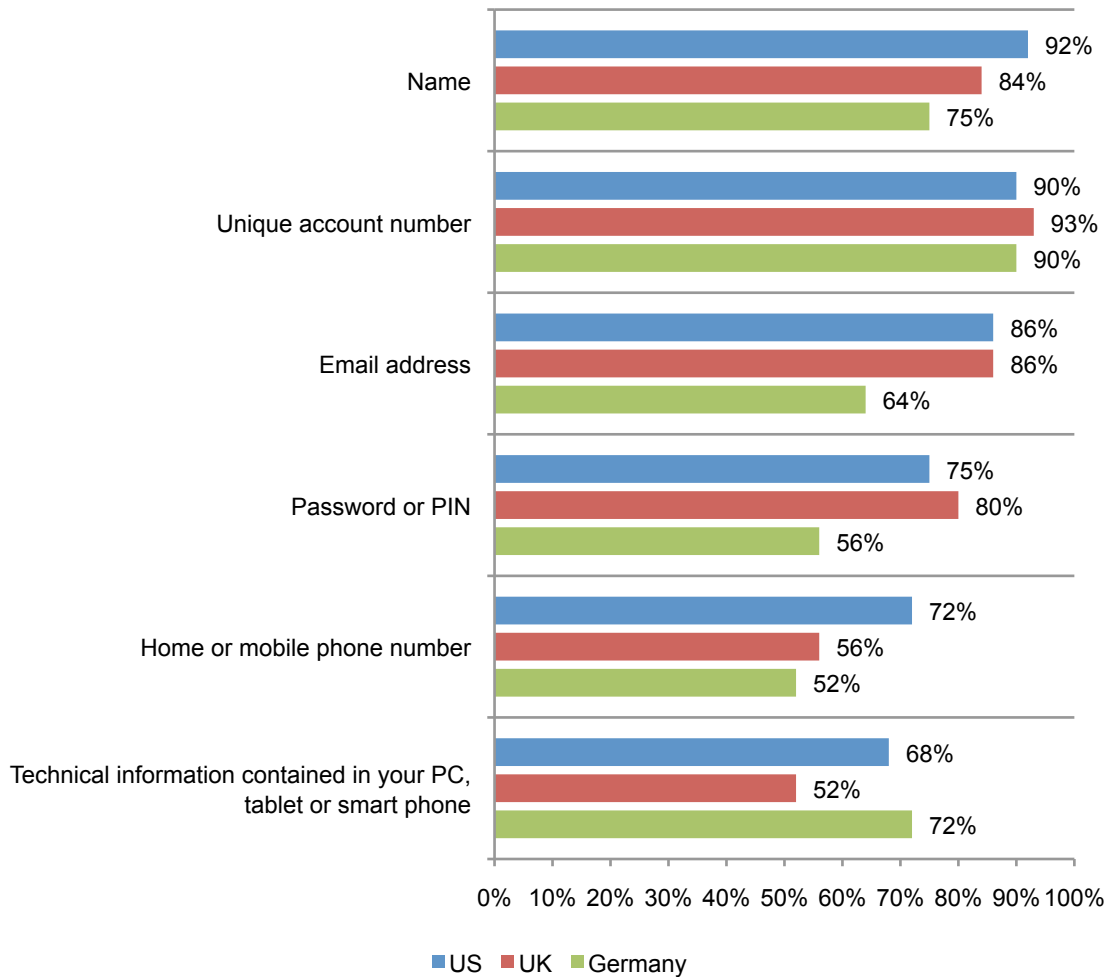
Consumers in all three countries would be willing to share the following information with a **government** organization: home address, unique account number and name, passport number and country of citizenship as shown in Figure 12.

Figure 12. Information willingly shared with a government organization
More than one response permitted
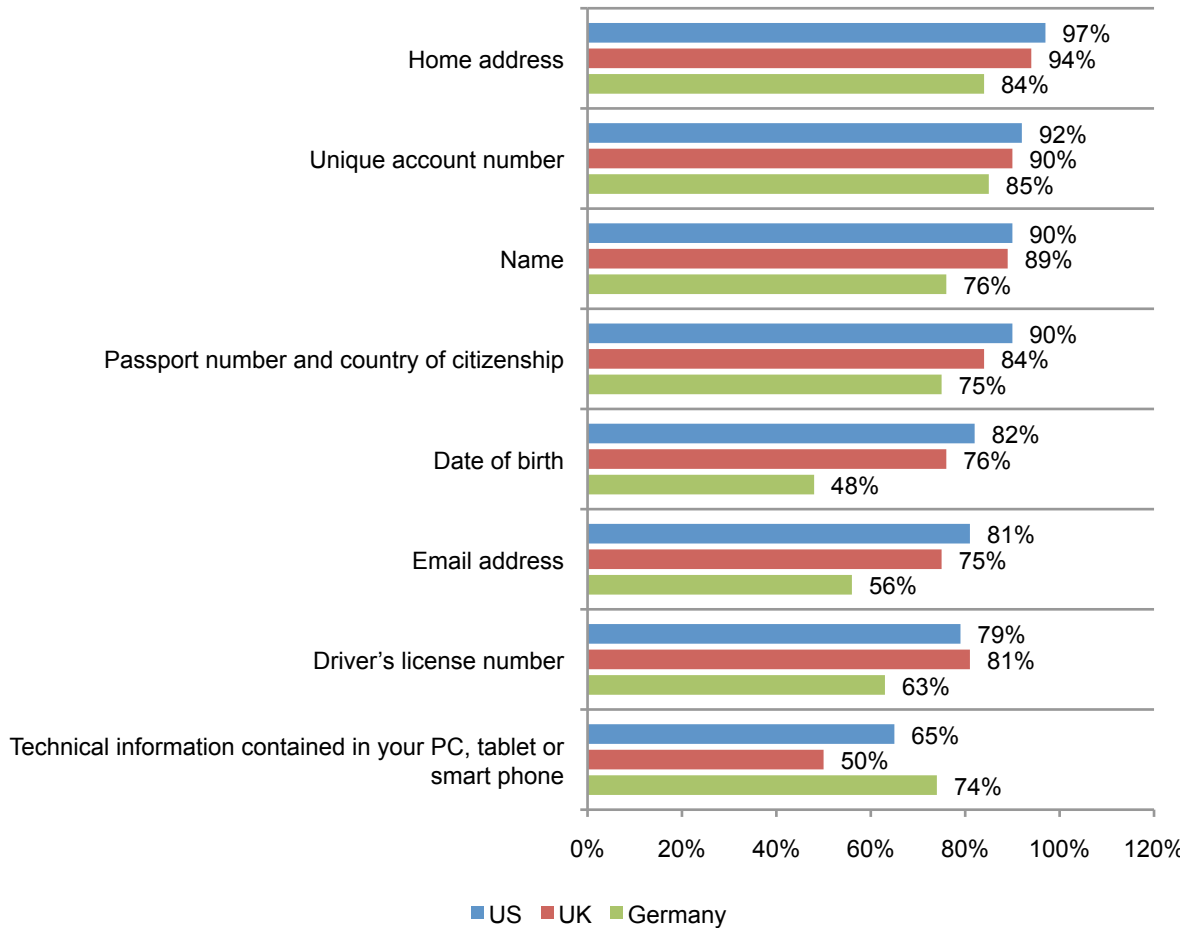
The majority of consumers would use a multi-purpose identity credential. According to Figure 13, a majority of consumers would consider using a multi-purpose identity credential to be able to secure access to data, systems and physical locations. In some cases, they would prefer if separate IDs were to be used for Internet and physical locations. Consumers in the UK express the highest "no" and "unsure" responses.

Figure 13. Acceptance of a multi-purpose identity credential

Legend: US, UK, Germany
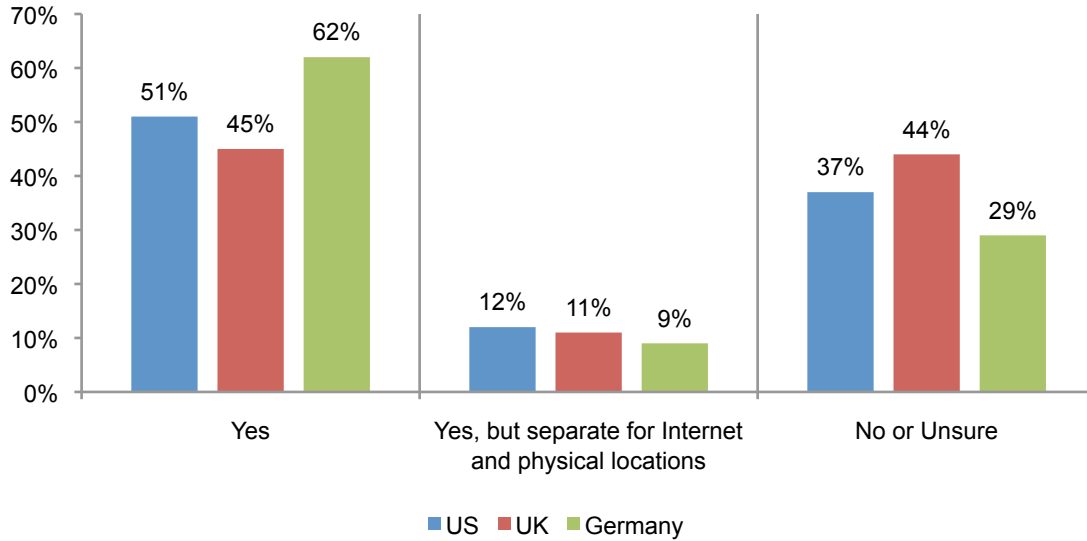
Consumers believe banks would be the best to safely issue and manage a multi-purpose identity credential. The majority of consumers would consider having a multi-purpose identity credential they could use in a variety of situations to confirm who they are. However, some consumers would like to have separate ID credentials for Internet and physical locations.

The five most trustworthy organizations according to consumers surveyed are: banking institutions, credit card and Internet payment providers, utilities, postal and delivery services, and law enforcement, as shown in Figure 14. Least trusted are educational institutions, Internet service providers and retailers. The complete list with frequency of response is shown in the appendix.

Figure 14. Organizations trusted to issue and manage a multi-purpose identity credential
1 = the most trusted to 15 = the least trusted organization
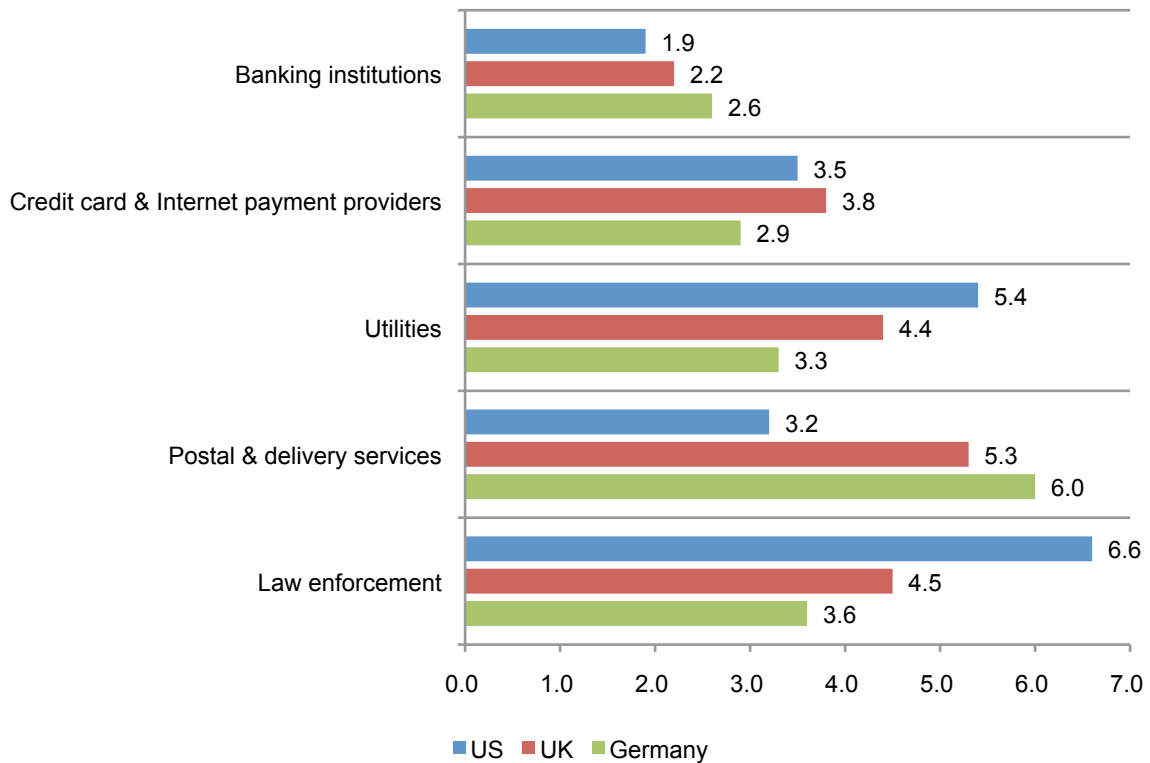
Consumers choose convenience for verification of their identity. In all three countries, the primary reason consumers would like a multi-purpose identity credential is convenience, as shown in Figure 15. Unlike consumers in the US and UK, the majority of German consumers believe such identification would improve security. Fewer consumers see ease of use and enhanced privacy as benefits.

Figure 15. Convenience is the top reason for a multi-purpose identity credential
Two choices permitted
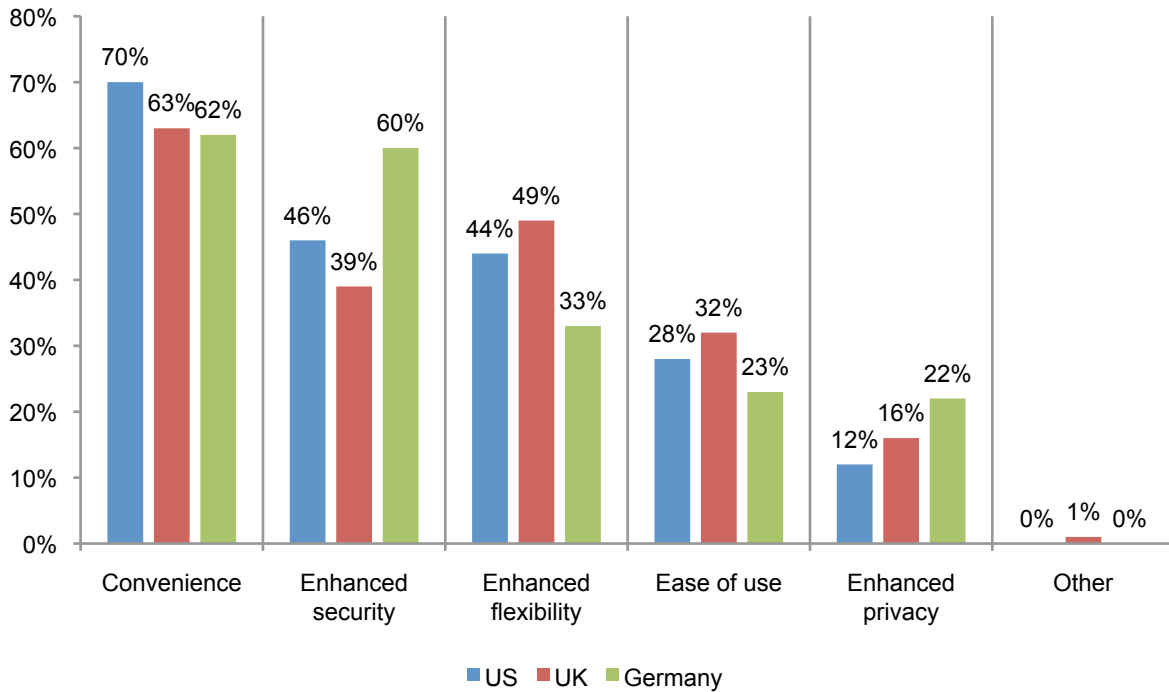
Consumers who are unsure or do not like the idea of such a credential believe that it will permit others to link their activities to the Internet, as shown in Figure 16. This is followed by concerns that the credential also would be used for access to physical locations. German consumers do not want to use the same credential for all online activities and believe the centralization of their identity yields too much power to the issuers of this credential. As shown in the figure, only a small percentage are concerned with having all of their identification on one card.

**Figure 16. Concerns about having a single ID**
Two choices permitted
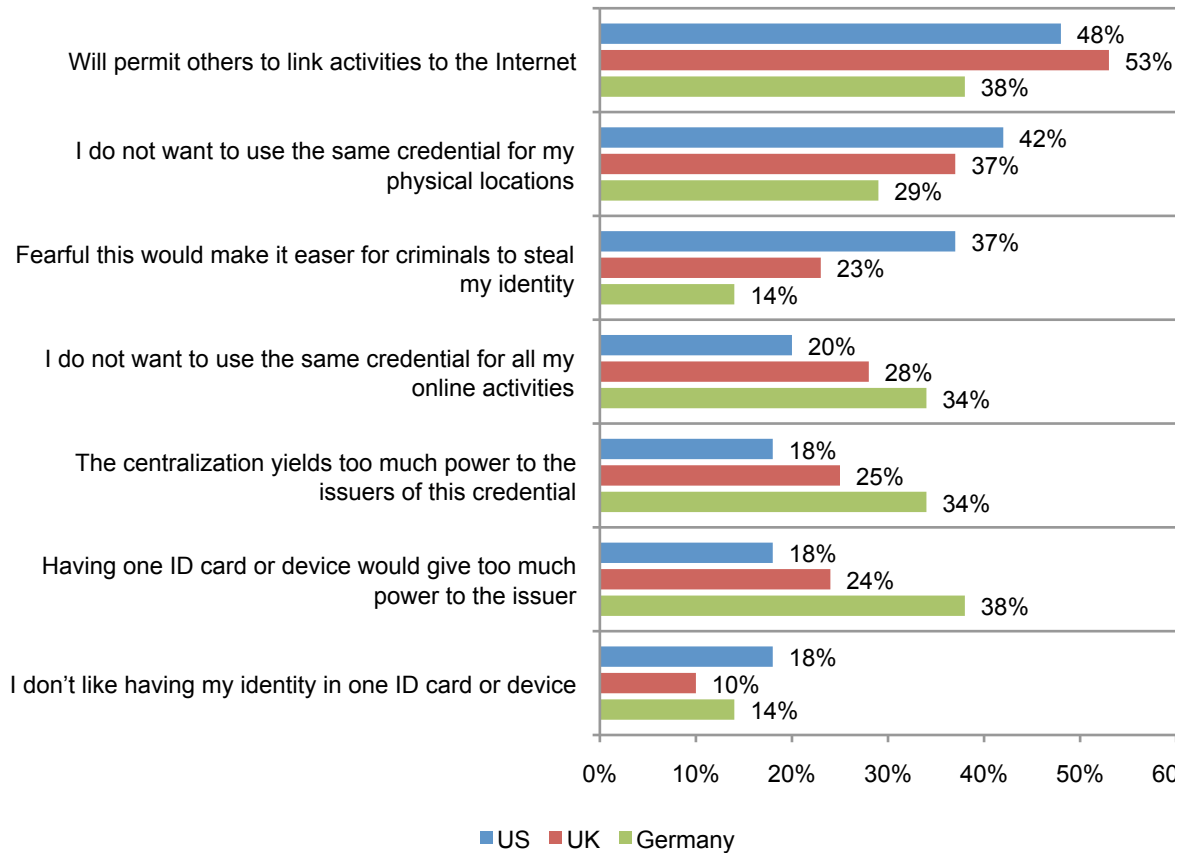
How consumers would use a multi-purpose credential. As revealed in Figure 17, consumers would like to use the multi-purpose identity credential to provide access to the following functions: public transportation carriers, Internet, social networks, government records, international travel and mobile devices. The majority of respondents in UK and Germany would like the credential to provide access to health records.

Figure 17. Multi-purpose identity credential use
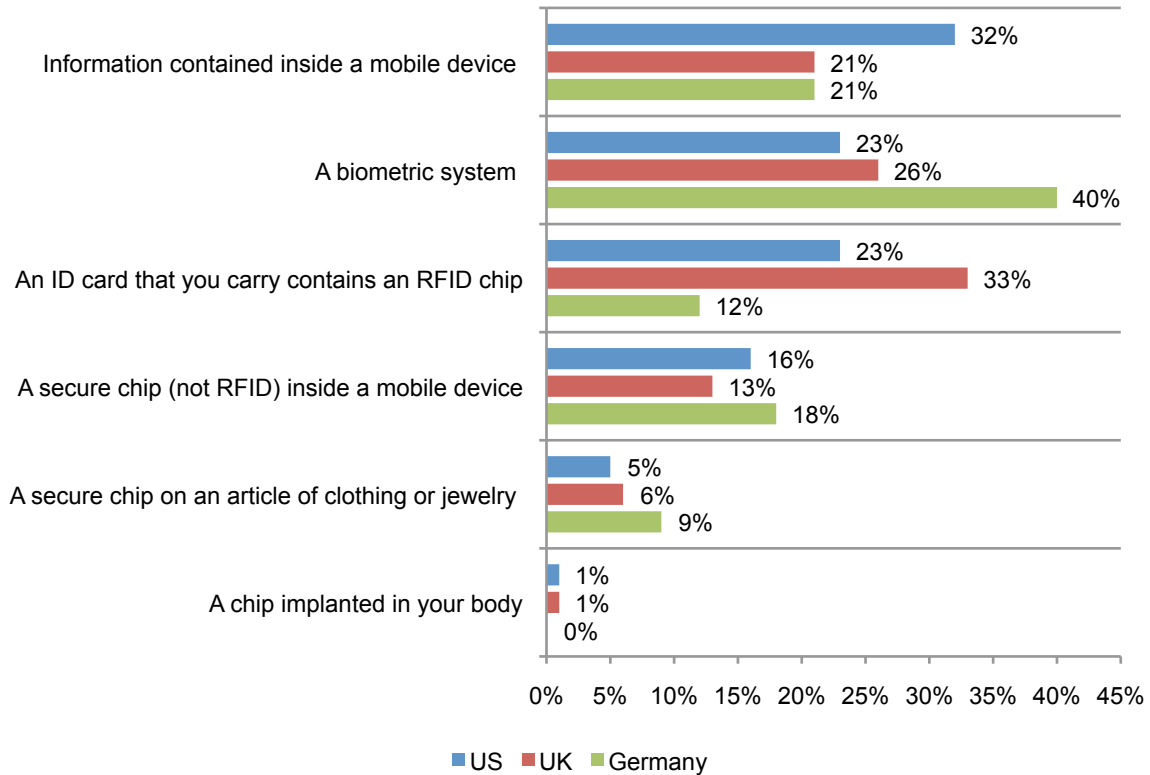More than one response permitted
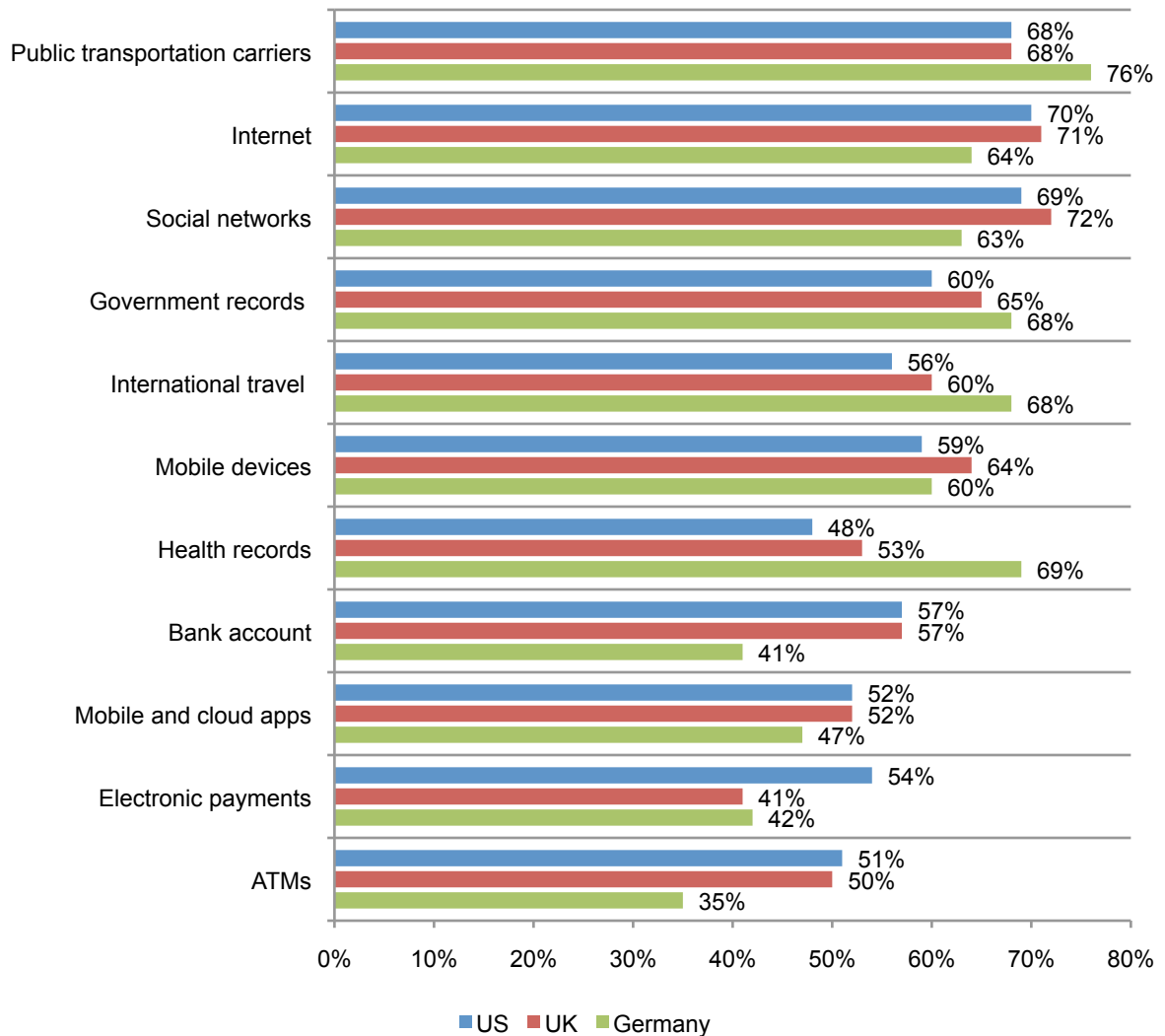
There are country differences in the preferred devices for managing multi-purpose credentials and no clear consensus as to what device would be most preferable. Almost one-third of US consumers prefer that their mobile device such as a phone, laptop or tablet contain their personal information.

Forty percent of German consumers prefer a biometric system (i.e. voice, fingerprint, retina scan, facial scan and others) and one-third of UK consumers select an ID card that contains an RFID chip, as shown in Figure 18. Very few would like a secure chip that is in an article of clothing or jewelry or implanted in the body.

Figure 18. Preferred device to manage a multi-purpose identity credential
Only one choice permitted

Legend: ■ US ■ UK ■ Germany

| Category	US	UK	Germany
Information contained inside a mobile device	32%	21%	21%
A biometric system	23%	26%	40%
An ID card that you carry contains an RFID chip	23%	33%	12%
A secure chip (not RFID) inside a mobile device	16%	13%	18%
A secure chip on an article of clothing or jewelry	5%	6%	9%
A chip implanted in your body	1%	1%	0%

The majority of consumers in the UK and Germany would not permit an organization to use the personal information it collects to verify their identity for other purposes, such as promoting products and services to them as revealed in Figure 19. US consumers seem to be slightly more receptive to organization's use of their personal information for other purposes but would like to be able to have more control over how their information would be used to offer services.

Figure 19. Are organizations permitted to use personal information for other purposes?

US UK Germany
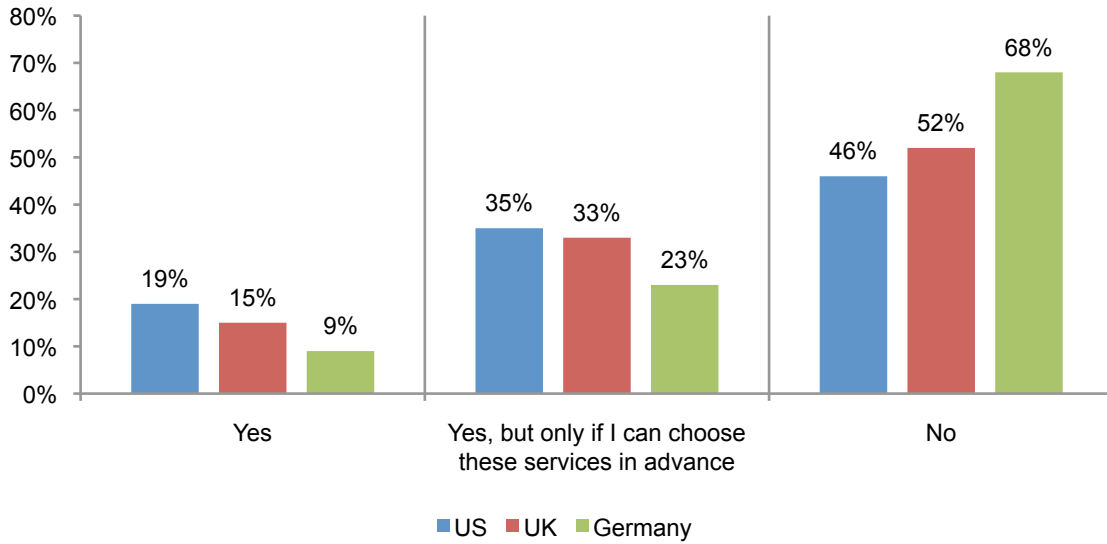
According to Figure 20, the majority of consumers believe it is acceptable for a trusted organization such as their bank, credit card companies, health care provider, telecom, email provider or governmental organization to use biometrics such as voice or fingerprints to verify their identity. However, some of these respondents say this is acceptable only if the biometric data is not accessible to the organization. The majority also would permit the biometric to be stored at a service provider.

Figure 20. Can a trusted organization use biometrics to authenticate consumers?
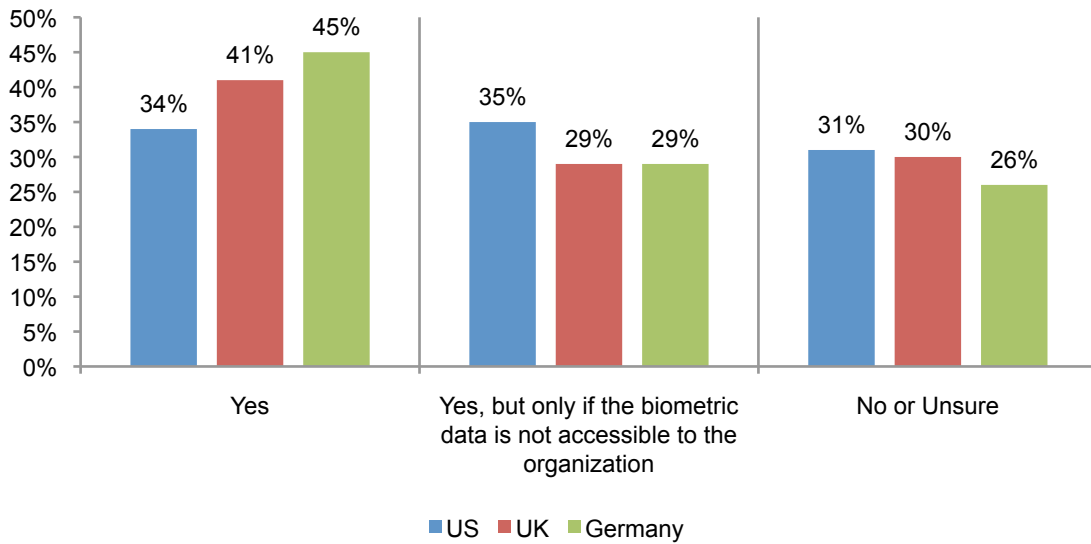
The top two types of biometric authentication methods most preferred are voice recognition and facial scan as shown in Figure 21. This is especially the case among German consumers. Hand geometry, fingerprints and eye scans are not as popular.

Figure 21. Preferred biometric methods
Two responses permitted
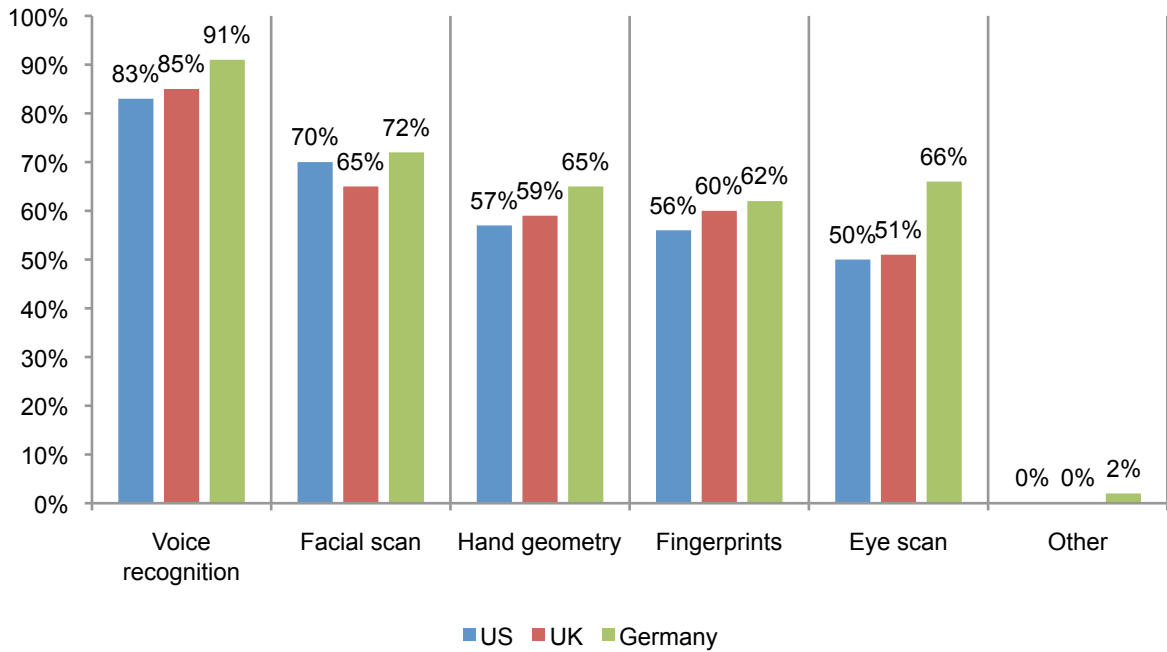
Consumers want secure authentication and verification when sharing a computer with others.
The majority of consumers believe it is important to have authentication that securely verifies their
identity on devices that are shared with other (multiple) users. Figure 22 reveals activities that
consumers would perform on computers shared with others include search & information gathering
and social networking. The complete list of activities is shown in the appendix.

Figure 22. Activities performed on a shared computer
More than one response permitted
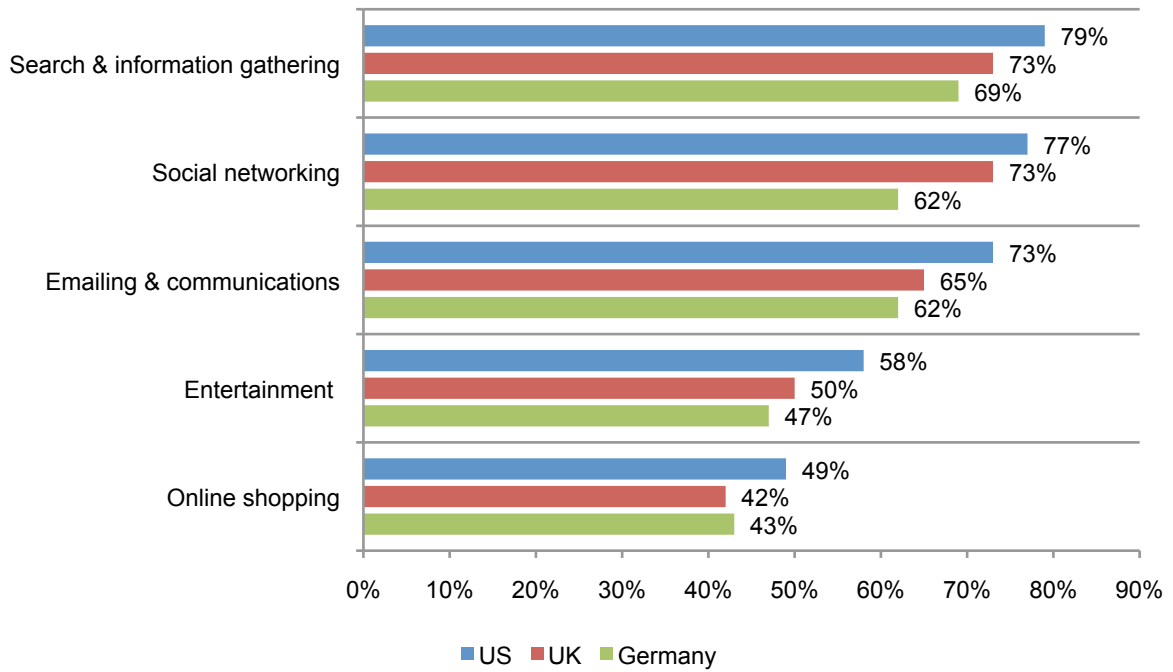
If consumers share log on credentials, would this affect the types of activities they would engage in? The majority of consumers in all countries would be comfortable conducting online searches. In the US, the majority would engage in entertainment such as music or gaming and German consumers would upload videos when sharing log on credentials (Figure 23).

Figure 23. Activities performed using a shared logon credential
More than one response permitted
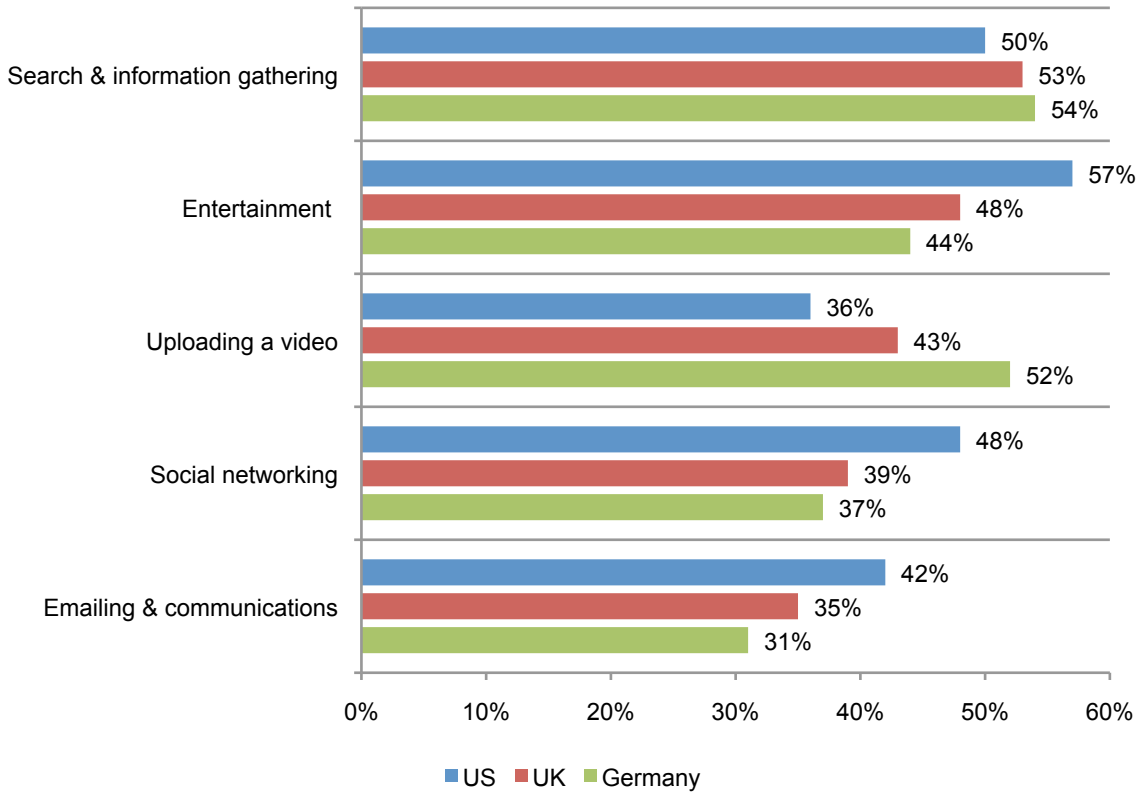
Part 3. Methods & Limitations

Table 1 reports the sample response for three separate country samples. The sample response for this study was conducted in November 2012. Our consolidated sampling frame of consumers in all countries consisted of 47,625 individuals who are 18 years or older. From this sampling frame, we captured 2,292 returns of which 134 were rejected for reliability issues. Screening removed another 234 returns, resulting in a final sample of 1,924 or a 4 percent response rate.

Table 1. Survey response	US	UK	Germany	Total
Sampling frame	19,300	14,080	14,245	47,625
Total returns	915	665	712	2,292
Total rejections	56	40	38	134
Screened responses	105	56	73	234
Final sample	754	569	601	1,924
Response rates	3.9%	4.0%	4.2%	4.0%

According to Table 2, the majority of respondents have at the minimum attended a university or college.

Table 2. The highest level of education attained	US	UK	Germany
High school	20%	22%	23%
Vocational	21%	26%	19%
Attended university or college	26%	24%	28%
University or college degree	23%	19%	20%
Post Graduate	9%	8%	8%
Doctorate	1%	1%	2%
Total	100%	100%	100%

More than half of respondents are employed at least on a part-time basis, as shown in Table 3.

Table 3. Employment status	US	UK	Germany
Full time employee	45%	44%	56%
Part time employee	12%	10%	10%
Business owner	8%	6%	5%
Homemaker	12%	14%	9%
Student	8%	8%	7%
Retired	5%	8%	7%
Military	1%	0%	0%
Unemployed	9%	10%	6%
Total	100%	100%	100%

The majority of respondents reported their income to be between $20,000 and $80,000 as revealed in Table 4.

Table 4. Household income (US$)	US	Converted to US$ Dollars	
		UK	Germany
< $20,000	14%	11%	9%
$20,000 to $40,000	19%	18%	17%
$41,000 to $60,000	20%	23%	23%
$61,000 to $80,000	18%	23%	25%
$81,000 to $100,000	15%	14%	14%
$101,000 to $150,000	7%	6%	8%
$151,000 to $250,000	5%	4%	3%
> $250,000+	2%	1%	1%
Total	100%	100%	100%
Extrapolated household income in US dollars	$68,410	$65,790	$67,010
Extrapolated household income in original currency	$68,410	£41,442	52,673 €

According to Table 5, more than half of respondents are between the ages of 18 and 45.

Table 5. Age range	US	UK	Germany
18 to 25	21%	22%	22%
26 to 35	25%	24%	25%
36 to 45	23%	27%	26%
46 to 55	15%	12%	13%
56 to 65	13%	12%	11%
65+	3%	3%	3%
Total	100%	100%	100%
Extrapolated age of respondents	38.5	37.9	37.7

Part 4. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to many consumer-based surveys.

▪ <u>Non-response bias</u>: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of adult-aged consumers located in all regions of the United States, United Kingdom and Germany resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

▪ <u>Sampling-frame bias</u>: The accuracy is based on contact information and the degree to which the sample is representative of individuals who access the Internet more than 10 hours per week. We also acknowledge that the results may be biased by external events such as media coverage at the time we fielded our survey.

We also acknowledge bias caused by compensating respondents to complete this research within a holdout period. Finally, because we use a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

▪ <u>Self-reported results</u>: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that certain respondents did not provide accurate responses.

Appendix: Detailed Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in November 2012.

Survey response	US	UK	Germany
Sampling frame	19,300	14,080	14,245
Total returns	915	665	712
Total rejections	56	40	38
Screened responses	105	56	73
Final sample	754	569	601
Response rates	3.9%	4.0%	4.2%

Part 1. Screening Questions			
S1. How many hours each week do you spend using the Internet (including time doing social media)?	US	UK	Germany
< 10 hour (Stop)	53	63	49
11-20 hours	228	153	160
21 to 40 hours	353	289	303
> 40 hours	281	160	200
Total	915	665	712
Median hours	29	28	29

S2.Which of the following online activities do you do in a typical week?	US	UK	Germany
Online shopping	553	409	413
Blogging	156	121	103
Online banking	235	206	241
Search & information gathering	699	508	519
Entertainment such as music or gaming	505	407	418
Emailing & communications	693	511	561
Obtaining government (e-citizen) services	228	209	280
Social networking (such as Facebook, Twitter, LinkedIn)	659	433	480
Uploading a video	134	119	98
None of the above (Stop)	108	33	62
Total	862	602	663

Part 2. Attributions: Please respond to each one of the eight (8) statements using the five-point scale provided below each item. Strongly agree and Agree responses combined.	US	UK	Germany
Q1. Most authentication failures happened because I forgot my password, username, or a response to a fact-based question (such as mother's maiden name).	63%	55%	51%
Q2. Most authentication failures happened because the organization or website had glitches or inaccuracies within their systems or identity verification procedures.	38%	44%	48%
Q3. Most websites I use have authentication procedures that can be trusted to safeguard my sensitive or confidential information.	49%	48%	56%
Q4. I do not use websites that appear to have inadequate authentication and identity verification procedures.	35%	39%	52%
Q5. I do not trust systems or websites that **only** rely on passwords to identify and authenticate users or consumers.	46%	45%	65%
Q6. I do not trust systems or websites that do not force me to change my password on regular intervals.	38%	37%	46%
Q7. I prefer authentication procedures that verify my identity without requiring me to share personal information such as my name, address, email and so forth.	67%	72%	78%
Q8. I do not trust systems or websites when identity and authentication procedures appear too easy.	46%	48%	61%
Average	48%	49%	57%

Part 3. Your experiences			
Q9. Following are 20 situations experienced by many people because of authentication failures and other related identification issues. Using the following scale, please select the appropriate number for each situation according to your actual experiences over the past 24 months. **Percentage of respondents who say it happened to them one or more times over the past 2 years.**	US	UK	Germany
Locked out of an Internet site because of an authentication failure	67%	66%	60%
Someone else used my logon credentials on a shared laptop or desktop computer	20%	12%	12%
Discontinued a relationship with a web merchant because of their poor authentication practices	22%	28%	25%
Waited a long time to have username or password reset	54%	53%	47%
Could not obtain funds from an ATM machine because of authentication failure	17%	10%	7%
Could not obtain perks on my loyalty card because of authentication failure	19%	16%	10%
Could not enter a secure location such as an airport or government building	20%	19%	13%
Could not use my PC, tablet or smart phone because of an authentication glitch	36%	32%	28%
Did not have the right authentication technology (such as a token) required to access a secure website	29%	29%	24%
Did not have the right authentication technology (such as a token) required to securely process a credit card or Internet payment (such as PayPal)	36%	40%	32%
Could not complete a loan or mortgage transaction	5%	3%	1%
Inadvertently provided user name and password to a spoofed (fake) website	43%	49%	37%
Experienced a data breach that involved the loss or theft of identity credentials such as username, password and other items that can be used to validate identity	35%	33%	17%
Experienced an identity fraud because criminals were able to seize identity credentials	7%	5%	2%
An imposter was able to misuse private information in my social media site (wall)	5%	8%	11%
Could not file for or obtain government benefits	9%	13%	16%
Could not obtain government documents	10%	12%	15%
Could not obtain medical services	17%	23%	24%
Forgot a password because it was too long or complex	69%	70%	49%
Forgot the standard response to a fact-based or test question used to authenticate	52%	50%	39%
Average	29%	29%	23%

Q10a. From the list below, please select the **top three** organizations that you feel do the best job for online validation.	US	UK	Germany
Airlines	10%	11%	12%
Banking institutions	61%	58%	65%
Credit card and Internet payment providers	50%	52%	54%
Telephone, wireless or cable services companies	11%	9%	10%
Health care providers	16%	17%	14%
Educational institutions	7%	6%	9%
Internet service providers	20%	23%	15%
Local or state government organizations	11%	11%	10%
Federal government organizations	11%	15%	12%
Postal and delivery services	14%	12%	9%
Retailers	25%	23%	28%
Social media	36%	31%	37%
Tax authorities	17%	20%	15%
Law enforcement	4%	7%	9%
Utilities	5%	5%	3%
Other	0	0	0
Total	300%	300%	300%

Q10b. From the list below, please select the **top three** organizations that you feel do the best job for physical validation.	US	UK	Germany
Airlines	47%	43%	52%
Banking institutions	45%	43%	28%
Credit card and Internet payment providers	19%	19%	13%
Telephone, wireless or cable services companies	30%	25%	31%
Health care providers	36%	38%	31%
Educational institutions	3%	3%	8%
Local or state government organizations	27%	35%	30%
Federal government organizations	36%	37%	42%
Postal and delivery services	21%	18%	21%
Retailers	5%	1%	7%
Tax authorities	4%	5%	9%
Law enforcement	21%	26%	21%
Utilities	5%	6%	6%
Other	0%	0%	1%
Total	300%	300%	300%

Part 4. Your preferences			
Q11a. What information are you willing to share about yourself with a **business** organization such as a bank, airline, telecom, retailer, social network to help the organization verify your identity? Please check all the data elements that you are willing to share for purposes of identity and authentication.	US	UK	Germany
Name	92%	84%	75%
Password or PIN	75%	80%	56%
Unique account number	90%	93%	90%
Email address	86%	86%	64%
Home address	69%	51%	45%
Home or mobile phone number	72%	56%	52%
Social Security number or National ID	35%	23%	15%
Digital photo	38%	40%	31%
Technical information contained in your PC, tablet or smart phone	68%	52%	72%
Amounts of recent purchases	45%	53%	28%
Driver's license number	53%	43%	28%
Date of birth	59%	43%	32%
Mother's maiden name	64%	47%	38%
Response to test questions	59%	56%	40%
Credit card or debit card number	36%	30%	23%
Passport number and country of citizenship	24%	20%	27%
Facial or retina scan	28%	33%	38%
Finger or thumbprint	34%	38%	49%
Voice print (recording)	52%	54%	69%
None of the above	5%	6%	10%
Average	54%	49%	44%

Q11b. What information are you willing to share about yourself with a **government** organization such as a post office, tax authority or law enforcement to help the organization verify your identity? Please check all the data elements that you are willing to share for purposes of identity and authentication.	US	UK	Germany
Name	90%	89%	76%
Password or PIN	70%	70%	49%
Unique account number	92%	90%	85%
Email address	81%	75%	56%
Home address	97%	94%	84%
Home or mobile phone number	73%	54%	45%
Social Security number or National ID	42%	23%	13%
Digital photo	30%	23%	11%
Technical information contained in your PC, tablet or smart phone	65%	50%	74%
Amounts of recent purchases	25%	17%	3%
Driver's license number	79%	81%	63%
Date of birth	82%	76%	48%
Mother's maiden name	65%	44%	39%
Response to test questions	54%	57%	45%
Credit card or debit card number	35%	21%	15%
Passport number and country of citizenship	90%	84%	75%
Facial or retina scan	11%	18%	35%
Finger or thumbprint	12%	23%	56%
Voice print (recording)	42%	35%	49%
None of the above	8%	7%	5%
Total	57%	52%	46%

Q12a. Would you consider having a **multi-purpose identity credential** that will be accepted by many organizations to verify who you are before providing secure access to data, systems and physical locations?	US	UK	Germany
Yes	51%	45%	62%
Yes, but separate for Internet and physical locations	12%	11%	9%
No or Unsure	37%	44%	29%
Total	100%	100%	100%

Q12b-1. If yes, what are your primary reasons for considering the multi-purpose identity credential? Top two choices.	US	UK	Germany
Convenience	70%	63%	62%
Ease of use	28%	32%	23%
Enhanced security	46%	39%	60%
Enhanced flexibility	44%	49%	33%
Enhanced privacy	12%	16%	22%
Other	0%	1%	0%
Total	200%	200%	200%

Q12b-2. If no or unsure, what are your concerns? Top two choices. Skip to Part 5.	US	UK	Germany
I do not want to use the same credential for my physical locations	42%	37%	29%
I do not want to use the same credential for all my online activities	20%	28%	34%
I am concerned that having one ID will permit others to link my activities to the Internet	48%	53%	38%
I don't like the idea of having my identity in one ID card or device	18%	10%	14%
Having one ID card or device would give too much power to the issuer	18%	24%	38%
The centralization of my identity yields too much power to the issuers of this credential	18%	25%	34%
I am fearful of this would make it easer for criminals to steal my identity	37%	23%	14%
Other	0%	0%	0%
Total	200%	200%	200%

Q13. Please check the functions that you would like a multi-purpose identity credential to provide access to	US	UK	Germany
Internet	70%	71%	64%
Social networks	69%	72%	63%
Bank account	57%	57%	41%
ATMs	51%	50%	35%
Mobile and cloud apps	52%	52%	47%
Electronic payments	54%	41%	42%
Public locations such as stadiums, transit stations or schools	48%	34%	40%
Government records (including voting systems)	60%	65%	68%
International travel (passport)	56%	60%	68%
Public transportation carriers (airplanes, trains and buses)	68%	68%	76%
Workplace locations	23%	15%	15%
Home	23%	21%	49%
Automobile	19%	14%	35%
Mobile devices including PC, tablet and smart phone	59%	64%	60%
Health records	48%	53%	69%
Other	2%	5%	2%
Total	759%	740%	774%

Q14. Please select the **one** device from the list below that you most prefer to manage your multi-purpose identity credential.	US	UK	Germany
An ID card that you carry contains an RFID chip	23%	33%	12%
Information contained inside a mobile device such as a laptop, tablet or smart phone	32%	21%	21%
A secure chip (that is not RFID) inside a mobile device such as a laptop, tablet or smart phone	16%	13%	18%
A secure chip (that is not RFID) on an article of clothing or jewelry (such as a bracelet or watch)	5%	6%	9%
A biometric system such as your voice, fingerprint, retina scan, facial scan and others	23%	26%	40%
A chip implanted in your body	1%	1%	0%
Other	0%	0%	0%
Total	100%	100%	100%

Q15. Please rank the following 15 organizations based on your level of **trust** in this organization's ability to safely issue and manage a multi-purpose identity credential. Please perform this ranking from 1 = the most trusted to 15 = the least trusted organization. If possible, please avoid tied rankings.	US	UK	Germany
Airlines	9.4	12.3	11.1
Banking institutions	1.9	2.2	2.6
Credit card and Internet payment providers	3.5	3.8	2.9
Telephone, wireless or cable services companies	4.9	7.9	3.3
Health care providers	4.6	3.9	8.1
Educational institutions	10.4	12.9	8.9
Internet service providers	12.6	13.8	15.2
Local or state government organizations	7.8	6.6	5.2
Federal/central government organizations	8.0	9.0	7.9
Postal and delivery services	3.2	5.3	6.0
Retailers	13.9	4.4	14.0
Social media	11.9	11.2	12.2
Tax authorities	8.4	10.5	8.3
Law enforcement	6.6	4.5	3.6
Utilities	5.4	4.4	3.3
Average rank	7.5	7.5	7.5

Q16. How important to you is the ability to use your multi-purpose identity credential in the different countries that you might visit for business or leisure?	US	UK	Germany
Essential	17%	19%	21%
Very important	21%	23%	30%
Important	26%	25%	29%
Not important	25%	20%	15%
Irrelevant	11%	13%	5%
Total	100%	100%	100%

Q17. Would you permit an organization to use the personal information it collects to verify your identity for other purposes, such as promoting products and services to you?	US	UK	Germany
Yes	19%	15%	9%
Yes, but only if I can choose these services in advance	35%	33%	23%
No	46%	52%	68%
Total	100%	100%	100%

Q18a. Is it acceptable for a trusted organization such as your bank, credit card company, health care provider, telecom, email provider or governmental organization to use biometrics such as your voice or fingerprints to verify your identity?	US	UK	Germany
Yes	34%	41%	45%
Yes, but only if the biometric data is not accessible to the organization.	35%	29%	29%
No or Unsure	31%	30%	26%
Total	100%	100%	100%

Q18b. If yes, what type of biometric authentication method would be most acceptable to you? Top two choices	US	UK	Germany
Voice recognition	83%	85%	91%
Facial scan	70%	65%	72%
Eye (iris) scan	50%	51%	66%
Fingerprints	56%	60%	62%
Hand geometry	57%	59%	65%
Other	0%	0%	2%
Average	53%	53%	60%

Q18c. For purposes of your convenience, would you permit your biometric (such as a fingerprint) to be stored at your service provider (i.e., telecom, email provider, and others)?	US	UK	Germany
Yes	66%	64%	58%
No or Unsure	34%	36%	42%
Total	100%	100%	100%

Q19. Do you expect certain organizations to have stronger authentication and identity verification methods than others?	US	UK	Germany
Yes	82%	78%	89%
No or Unsure	18%	22%	11%
Total	100%	100%	100%

Q20. In your experience, which organizations have **very strong** authentication and identity verification methods? Please select all that apply.	US	UK	Germany
Airlines	49%	42%	34%
Banking institutions	87%	94%	97%
Credit card and Internet payment providers	76%	75%	65%
Telephone, wireless or cable services companies	56%	60%	58%
Health care providers	72%	52%	58%
Educational institutions	23%	19%	39%
Internet service providers	23%	25%	15%
Local or state government organizations	45%	56%	58%
Federal government organizations	39%	41%	54%
Postal and delivery services	69%	56%	54%
Retailers	23%	49%	20%
Social media	19%	20%	16%
Tax authorities	68%	71%	72%
Law enforcement	85%	81%	83%
Utilities	45%	46%	42%
Average	52%	52%	51%

Q21. How important is authentication that securely verifies your identity on devices that are shared with other (multiple) users?	US	UK	Germany
Very important	25%	23%	21%
Important	34%	35%	30%
Somewhat important	19%	21%	23%
Not important	11%	12%	13%
Irrelevant	11%	9%	13%
Total	100%	100%	100%

Q22a. What activities would you **perform** on computer shared with others (multiple users)?	US	UK	Germany
Online shopping	49%	42%	43%
Blogging	28%	29%	33%
Online banking (including mobile payments)	21%	20%	18%
Search & information gathering	79%	73%	69%
Entertainment such as music or gaming	58%	50%	47%
Emailing & communications	73%	65%	62%
Obtaining government (e-citizen) services	45%	47%	50%
Social networking	77%	73%	62%
Uploading a video	39%	43%	52%
None of the above	25%	28%	21%
Average	49%	47%	46%

Q22b. What activities would you **perform** using a shared account (with shared logon credentials)?	US	UK	Germany
Online shopping	38%	27%	30%
Blogging	23%	25%	29%
Online banking (including mobile payments)	5%	8%	4%
Search & information gathering	50%	53%	54%
Entertainment such as music or gaming	57%	48%	44%
Emailing & communications	42%	35%	31%
Obtaining government (e-citizen) services	23%	25%	26%
Social networking	48%	39%	37%
Uploading a video	36%	43%	52%
None of the above	22%	26%	20%
Average	34%	33%	33%

Q23a. **Has this ever happened to you?** You wanted to perform an online transaction (such as buying a product or obtaining a service) but couldn't do so because of an (such as buying a product or obtaining a service) but couldn't do so because of an authentication failure on the website.	US	UK	Germany
Very frequently	20%	21%	19%
Frequently	26%	29%	34%
Not frequently	35%	36%	29%
Rarely	14%	10%	11%
Never	5%	4%	7%
Total	100%	100%	100%

Q23b. If you chose very frequently or frequently, how frustrating was this situation to you?	US	UK	Germany
Very frustrating	44%	41%	38%
Frustrating	31%	30%	33%
Somewhat frustrating	12%	13%	15%
Not frustrating	5%	8%	9%
Unsure	8%	8%	5%
Total	100%	100%	100%

Part 5. Sample demographics

D1. What computing devices do you own or extensively use?	US	UK	Germany
Desktop	65%	68%	61%
Laptop	69%	63%	70%
Tablet	38%	32%	39%
Smart phone	48%	56%	63%
None	3%	4%	2%
Total	223%	223%	235%

D2. Do you use one or more of the computing devices selected in D1 in the workplace (BYOD)?	US	UK	Germany
Yes	46%	44%	50%
No	54%	56%	50%
Total	100%	100%	100%

D3. If you use a smart phone, what is the device type?	US	UK	Germany
Apple	43%	39%	33%
Android	32%	39%	40%
Windows Mobile	10%	11%	13%
Blackberry	15%	10%	12%
Other	0%	1%	2%
Total	100%	100%	100%

D4. What is your highest level of education attained?	US	UK	Germany
High school	20%	22%	23%
Vocational	21%	26%	19%
Attended university or college	26%	24%	28%
University or college degree	23%	19%	20%
Post Graduate	9%	8%	8%
Doctorate	1%	1%	2%
Total	100%	100%	100%

D5. What best describes your employment status?	US	UK	Germany
Full time employee	45%	44%	56%
Part time employee	12%	10%	10%
Business owner	8%	6%	5%
Homemaker	12%	14%	9%
Student	8%	8%	7%
Retired	5%	8%	7%
Military	1%	0%	0%
Unemployed	9%	10%	6%
Total	100%	100%	100%

D6. Approximately, what is your household income (US$)?		Converted to US$ Dollars	
	US	UK	Germany
< $20,000	14%	11%	9%
$20,000 to $40,000	19%	18%	17%
$41,000 to $60,000	20%	23%	23%
$61,000 to $80,000	18%	23%	25%
$81,000 to $100,000	15%	14%	14%
$101,000 to $150,000	7%	6%	8%
$151,000 to $250,000	5%	4%	3%
> $250,000+	2%	1%	1%
Total	100%	100%	100%
Extrapolated household income in US dollars	$68,410	$65,790	$67,010
Extrapolated household income in original currency	$68,410	£41,442	52,673 €

D7. Your age range?	US	UK	Germany
18 to 25	21%	22%	22%
26 to 35	25%	24%	25%
36 to 45	23%	27%	26%
46 to 55	15%	12%	13%
56 to 65	13%	12%	11%
65+	3%	3%	3%
Total	100%	100%	100%
Extrapolated age of respondents	38.5	37.9	37.7

D8. Please check one.	US	UK	Germany
Female	52%	53%	50%
Male	48%	47%	50%
Total	100%	100%	100%

D9. Are you head of household?	US	UK	Germany
Yes	51%	49%	48%
No	49%	51%	52%
Total	100%	100%	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

Ponemon Institute LLC
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO),** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.