RUSSIAN INTERNET USERS' PRIVACY:
A STUDY OF ATTITUDES AND BEHAVIOR

A THESIS

SUBMITTED TO THE

STANFORD PROGRAM IN INTERNATIONAL LEGAL STUDIES

AT THE STANFORD LAW SCHOOL,

STANFORD UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF THE SCIENCE OF LAW

Advised under the faculty supervision of Professor Mark A. Lemley

By

Serhiy Hovyadinov

May, 2014

ABSTRACT

There is no sufficient empirical data on Russian Internet users' level of concern, their attitudes about online privacy, or their corresponding behavior. This research tries to remedy the shortage.

As the study demonstrates, the level of privacy concern in Russia is rather mixed: users are divided equally on whether they feel worried or not about the confidentiality of their personal data online. They also don't demonstrate a clear trust preference in online or offline environments as far as the protection of their data is concerned. Their level of worry about online privacy in the last year has significantly increased, and that increase could have been caused by media coverage of many recent privacy leaks.

Factors like frequency of the Internet use, age, material status and education have an effect on users' attitude and behavior. For example, despite a common perception that young people do not care about their privacy, there is evidence that the younger generation is not indifferent to their privacy and their identity. Users with a higher material status tend to feel less worried about their privacy, but at the same time they are more likely to take certain actions to protect their data.

Finally, the paper suggests several regulatory and educational measures that would help users make informed decisions, and offers some ideas to businesses to adjust their data gathering practices.

ACKNOWLEDGMENTS

I feel blessed to have met so many talented and remarkable individuals here at Stanford, both my professors and fellow students from SPILS and JSD programs. There are many people who contributed in one way or another and helped me finish this study, and it is hard to express in a few short paragraphs the gratitude I owe to all of them. I will try to do my best.

First, I would like to thank my advisor, Prof. Mark A. Lemley for his patience, availability, attentive supervision and very insightful advice at various junctions of my research that helped me develop a broader perspective to my thesis.

I am grateful to Prof. Deborah R. Hensler for her help with unraveling the intricacies of empirical legal research and her insightful advice on designing my survey.

My sincere thanks must also go to Sergio Puig, SPILS Teaching Fellow. His attention to my work and great assistance from the very start (those painful moments of finalizing my research topic) until the very end have been instrumental.

This study would not have happened if the Fund Public Opinion – Russian polling organization - did not agree to include my survey questions into one of its omnibuses. I am very grateful to Ms. Svetlana Borisova for helping make it possible.

Very special thanks are due to my "JSD mentor" Fernan Restrepo for his moral support, wise advice and for making the world of statistics look less formidable. I would also like to thank my many SPILS and JSD friends for their comments and camaraderie.

Finally, I thank with love my parents, my sister, my wife, and my kids for their love and incredible support, and for keeping me sane and focused during the last year despite anything.

TABLE OF CONTENTS

1. INTRODUCTION

One of the most notable changes in Russian society in the last decade has been the emergence and growth of the Internet and e-commerce. The market has grown at an amazing speed, and there are now more than 66 million Internet users in Russia alone. That figure gives Russia the biggest Internet population in Europe, and the growth is going to continue in the near future.[1]

Increasingly, international companies like Facebook, Twitter, and Google are reaching out across borders to gain access to the Russian market. However, differences in culture and national regulation have created some challenges, including the need to adjust privacy practices in accordance with users' preferences and local legal requirements.

As local and foreign Internet businesses in Russia increase the collection and use of personal information, and as more media outlets report stories of privacy breaches, the regulation of online privacy in Russia is leaning more and more towards a stricter government regulatory and enforcement model.

The privacy regulatory model is generally driven by state, industry and user interests, and may fall under one of the three main models: government regulation, self-regulation, or co-regulation. There is a general consensus that government involvement in the regulation of privacy is closely associated with the level of privacy concern in a country. That concern often stems from the perception created by corporate privacy practices and media coverage of privacy issues.

[1] See, e.g., Olga Razumovskaya, *Russia's Internet Market Predicted to Post Double-Digit Growth*, Wall S. J., Oct. 18, 2013 (citing a study conducted by the Russian Association for Electronic Communications and the Higher School of Economics, that predicts that the Russian Internet market is likely to grow an average of 15%-20% per year to 2018), *available at* http://blogs.wsj.com/emergingeurope/2013/10/18/russias-internet-market-predicted-to-post-double-digit-growth/

Last year saw a new wave of privacy debate that was triggered by revelations regarding practices of the NSA by Mr. Snowden combined with the subsequent reports on security and privacy breaches appearing thereafter on a regular basis. This combination led state officials in many countries around the world to accuse major Internet companies like Google and Facebook of the violation of email privacy, misuse, and insufficient protection of personal data. The issue was particularly intense in Russia; not just because Mr. Snowden had chosen Russia as his shelter, but also because the local state officials had been openly frustrated by a lack of authority over foreign Internet companies operating in Russia for a long time. The leaks by Mr. Snowden presented a unique opportunity to justify and promote an even stricter government model, allegedly for the benefit of the Russian users. As a result of the debate and accusations, new policy initiatives and legislative proposals were introduced to strengthen the state's control over the use of personal data, with a stricter liability for its violation.

While the Russian officials are claiming that their new proposals are aimed primarily to address users' concerns and better protect their interests, there is no sufficient empirical data on Russian Internet users' level of concern, their attitudes about online privacy, or their corresponding behavior.

My research project aims to take an empirical look at the level of privacy concern in Russia, and obtain a baseline understanding of how Russian Internet users evaluate online privacy based on four aspects: attitude, awareness, behavior, and trust. In addition, I submit four hypotheses that will be tested over the course of the research. The hypotheses are:

1. Participants with more Internet experience will exhibit lower levels of privacy concern.
2. Younger audiences will demonstrate a different privacy risk attitude and behavioral pattern.

3. In a paternalistic (highly regulated) privacy model, users tend to put more blame on the government or Internet businesses than on themselves in case of privacy breaches.
4. The NSA / Snowden scandal last year affected users' attitudes.

This paper is organized as follows:

- Part I reviews theoretical framework and previous literature on various concepts of privacy, factors that contribute to the level of privacy concern, privacy related behavioral choices, and existing privacy regulation models. This part will also include a brief summary of the current privacy regulatory framework in Russia, characterizing it as a "strict government regulation" model.
- Part II will include a description of the researcher's methodology and approaches to the data analysis.
- Part III includes both the summary of the findings and a detailed analysis of the survey results utilizing various statistical methods.
- In Part IV, each of the four hypotheses is analyzed separately.
- Finally, the conclusions will be detailed in Part V.

This is the first survey and study of this scope on privacy in Russia, and I believe the empirical results and analysis presented here can become a foundation for any future debate on privacy regulation in Russia.

2. THEORETICAL FRAMEWORK AND LITERATURE REVIEW

"Privacy in the modern age has largely been an issue of physical walls—walls that protect our possessions, shield our secrets and provide a haven for lives that are different from our public personas. But the very nature of virtual life seems to rebel against this opacity… Privacy will never be the same".
Ashley Dunn 1996

"Privacy may be an anomaly"
Vint Cerf 2013

A. The concept of privacy

Trying to define "privacy" is an academic nightmare.[2] There is no universally agreed definition of what privacy is.[3] Under Westin's "control theory" of privacy, it is defined as the amount of control that individuals can exert over the type of information, and the extent of that information, revealed to others.[4] A "restricted access" view of privacy, proposed by Moor, regards privacy as a complex of situations in which information is authorized to flow to specific people, at specific times. Moor suggested that in a highly computerized culture, it is simply not possible to control all personal information that resides on computer systems around the world. Therefore, the best way to protect privacy is to make sure that the right people have access to relevant information at the right time.[5] Altman viewed privacy as the presence of forces for people to make themselves more or less accessible to others.[6]

Moloney used a combination of Westin and Altman theories as a basis to develop an online privacy theory, which she defines as, "the continuous process of negotiating, with relevant third parties, an optimum or acceptable level of disclosure of personal information in an online environment".[7] Under Moloney's theory, the desired level of privacy is a dynamic function.

---

[2] *See, e.g.,* Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34, 35 (1967) ("[T]he concept of privacy is infected with pernicious ambiguities."); Fred H. Cate & Robert Litan, *Constitutional Issues in Information Privacy*, 9 Mich. Telecomm. & Tech. L. Rev. 35, 37 (2002) ("[privacy] can mean almost anything to anybody.").
[3] *See generally* Daniel J. Solove, *Conceptualizing Privacy,* 90 CALIF. L. REV. 1087 (2002); Richard B. Parker, *A Definition of Privacy,* 27 RUTGERS L. Rev. 275, 277 (1974).
[4] Alan F. Westin, *Privacy and Freedom* 7 (1967).
[5] James H. Moor, *Towards a theory of privacy in the information age,* ACM SIGCAS Computers and Society vol. 27, 27-32 (1997).
[6] Irwin Altman, *Privacy Regulation: Culturally Universal or Culturally Specific?* Journal of Social Issues, 33: 66–84 (1977).
[7] Maria Moloney & Frank E. Bannister, Privacy Control Theory for Online Environments, *Proceedings of the 42nd Hawaii International Conference on System Sciences,* August 3, 2009, *available at*: http://ssrn.com/abstract=2227595.

Users may choose the amount of privacy they deem fit depending on the environment they operate in and their needs. A subjective decision-making process, influenced by an individual's personal characteristics and corresponding pressures from the external environment, impacts negotiation with third parties for the continuous protection of personal information. Users adjust their privacy preferences as they deem appropriate under particular circumstances. Once they have analyzed the online environment and the perceived risks involved, they can decide whether or not the need to enter into an online transaction outweighs the perception of the risk of submitting their personal information. Conversely, they can decide to remain anonymous and forego the transaction.[8] Thus, users choose the actions that bring them closest to their "optimal or acceptable level of privacy".[9]

Disassembled, I find Moloney's theory a useful foundation for my study because it incorporates several very relevant and distinct elements that will be further evaluated: user's choice (negotiating), trust (relevant third parties), and subjective attitude (optimum level of privacy).

B. Privacy as a cultural phenomenon: culturally universal or culturally specific?

Are privacy concerns universal across cultures? Is it plausible to expect that Russian users will demonstrate a very different attitude and privacy behavior compared to *e.g.* German or Australian users?

[8] The development of technology and market competition have demonstrated that in addition to the choice between disclosing information or foregoing the transaction altogether, users may also be either offered to pay to remain anonymous, or be paid to disclose personal data, which amounts to the same thing. As an example of such "new trend", a Dutch student Shawn Buckles put a bundle of his personal information, including emails, his browser history and personal calendar, up for an auction and sold it to the highest bidder for €350 (about $485). The auction was won by The Next Web – a technology media-company managing several initiatives focused on international technology news, business and culture. The auction site is available at http://www.shawnbuckles.nl/dataforsale/.

[9] Moloney & Bannister, *supra* at 6.

Westin examined privacy's value in a cross-cultural setting and submitted that at least four privacy-related features may turn out to be universal across cultures. First, individuals make use of social distance and avoidance rules in the course of social interaction. Second, individuals believe that they are never truly alone, most likely as a consequence of an underlying fear of isolation. Third, there is a tendency on the part of individuals to invade the privacy of others and on the part of society to make use of surveillance to prevent antisocial conduct. Finally, as society becomes more complex, physical and psychological opportunities for privacy tend to increase.[10]

Milberg et al. found the ranking order of privacy concerns – that is, how levels of concern about collection, unauthorized secondary use, improper access and errors are ranked, with an unauthorized secondary use reported to be of the most concern -- to be consistent across cultures.[11] They also proposed that citizens in highly individualistic countries exhibit a higher level of concern for privacy. Their assertion was based on prior work that found a societal norm associated with countries that strongly value individualism is the belief that everyone has the right to a private life. On the other end of the spectrum, in countries for which individualism is of lower importance, there is more of an acceptance for organizational practices that will intrude on one's private life.[12] Altman showed that even though all cultures value intimacy in some form and the need for privacy is more or less universal, behavioral mechanisms used to regulate desired levels of privacy may differ.[13] For example, in Russia, a country for which individualism

[10] Alan Westin, *The Origins of Modem Claims to Privacy*, in *Philosophical Dimensions of Privacy*, 56, 60-61 (1984).
[11] Sandra J. Milberg et al., *Information privacy: Corporate management and national regulation*, Organ. Sci. (2000) 11(1):35–37.
[12] Sandra J. Milberg et al., *Values, personal information privacy, and regulatory approaches*, Comm. ACM 38 (12) 65–74 (1995).
[13] Altman, *supra* at 77.

is of lower importance,[14] a public opinion can also have a far greater effect on the choice of privacy behavior model compare to other countries.[15]

C. Privacy choice and decision making

The decision to interact online in a manner that might put a user's privacy at risk and the strategies that user may deploy to handle such risk, are instances of decisions made under conditions of uncertainty.[16] There are two main theories in the economics literature with respect to decision making under uncertainty. The first one is "rational choice" or "rational decision making." Under this theory, the individual decision–maker chooses among alternatives in a way that aligns with his or her preferences and beliefs. This assumes that the decision–maker is both fully rational (able to formulate and chose among all alternatives) and provided with a sufficient amount of information.[17]

The other theory is based on "bounded rationality," later developed into "behavioral economics," and abandons some of the tenets of rational choice theory, i.e. that agents possess consistent preferences between alternatives, choose the utility maximizing option, discount future events consistently, and act upon complete information or known probability distributions for all possible events.[18] As part of this theory, Kahneman and Tversky formulated three

---

[14] Duane Goehner & Yale Richmond, *Russian / American Cultural Contrasts. Available at* http://www.goehner.com/russinfo.htm.

[15] *See, e.g.*, Fatyanov A.A., *Pravovoe obespechenie bezopasnosti informacii v Rossiyskoy Federacii* 219 (2001) *("Any sane person from the moment of awareness of himself as a person exists as if in two parallel planes - to himself he appears in one incarnation, to others, to external environment – in another. Vast majority of people are not eager to demonstrate their inner world, their intimate nooks and that the totality of the information for various reasons a person wishes to hide from others <...> More in-depth insight into the causes of such a behavioral model of a man is the subject matter of psychology. For jurisprudence what important is that such behavioral model is a common repetitive behavior – a norm. Moreover, the deviation from this norms is perceived negatively by society and, moreover, in some cases, a loss of their individual "informational shell" can lead to tragic consequences: crime or suicide"*).

[16] Maria Moloney & Valerio Poti, *A Behavioral Perspective on the Privacy Calculus Model* 2 (2013), *available at* http://ssrn.com/abstract=2310535.

[17] *See, e.g.*, Paul Anand, *Foundations of Rational Choice Under Risk (*3rd ed. 2002).

[18] *See, e.g.*, Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?* in *Digital Privacy: Theory, Technologies, and Practices* (2008).

general-purpose heuristics that underlie many intuitive judgments under uncertainty:[19] "availability,"[20] representativeness,"[21] and "anchoring and adjustment."[22]

Moloney and Poti analyzed practical effects of ambiguity aversion and heuristic-driven biases in privacy risk handling behavior and found that in the face of ambiguity, both the willingness to disclose personal information and the propensity to engage in privacy risk handling behavior decrease; while an individual's experience regarding recent privacy breaches increases their privacy risk behavior (the effect of availability bias and representativeness).[23]

Last year saw an avalanche of privacy breach media coverage in Russia that was triggered by Mr. Snowden's revelations regarding NSA practices and unauthorized access to personal data. Subsequent reports on security and privacy breaches appeared thereafter on a regular basis.[24] Thus, I hypothesize the following:

Hypothesis 1: The *NSA / Snowden scandal affected users' attitude about online privacy.*

---

[19] Amos Tversky & Daniel Kahneman, *Judgment under uncertainty: Heuristics and biases*, Science 185.4157 (1974): 1124-1131.

[20] For example, many people may rely on media to formulate their opinion about privacy risk. If the media in Russia following the NSA scandal tends to report that American companies disrespect users' privacy and disclose personal data of Russian users to the US authorities, and not cover any surveillance activity of the Russian law enforcement, users who rely on availability heuristics recall instances related to the NSA and American Internet companies more readily than those related to their Russian counterparts. On the effect of this heuristic on my study see section "Limitations".

[21] Representativeness is *"the degree to which [an event] (i) is similar in essential characteristics to its parent population, and (ii) reflects the salient features of the process by which it is generated"*. (Kahneman, Tversky, Daniel, Amos (1972). "Subjective probability: A judgment of representativeness". In Kahneman, Slovic, Tversky. *Judgment under uncertainty: Heuristics and biases*. Cambridge: Cambridge University Press.). For example, people have long believed that ulcers were caused by stress, due to the representativeness heuristic, when in fact it is bacteria that causes ulcers. http://en.wikipedia.org/wiki/Representativeness_heuristic.

[22] Anchoring is a heuristic under which individual places significant weight on the first piece of information offered (the "anchor") when making decisions, e.g., price tag on a car is a typical example of an anchor which then sets the standard for the rest of the negotiations. According to Tversky and Kahneman, once an anchor is set, people adjust away from it insufficiently, resulting in their final guess being closer to the anchor than it would be otherwise. (Tversky, A., & Kahneman, D., *Advances in prospect theory: Cumulative representation of uncertainty.* Journal of Risk and Uncertainty, 5, 297–323 (1992)). In a privacy world, one may think of a situation when buyers in a shop are asked by a cashier to provide a "phone number or email address" without always recognizing that (a) this is optional, and (b) the choice between "phone number" and "email address" is artificially set as an anchor, so that it is easier for the buyer to reject one and not both options.

[23] Moloney & Poti, *Supra* at 87.

[24] According to the report by the Russian data security company InfoWatch, there were totally 109 personal data leaks reported in the Russian media in 2013, which represents more than a two times increase compare to 2012. The report is available at https://www.infowatch.ru/analytics/reports/5538

D. Privacy calculus

A distinct trait in the privacy decision-making research that also utilizes economic findings, including those offered by Kahneman and elaborated upon by behavioral economists, is the suggestion, implicit or explicit, that privacy is not an absolute, but can instead be assigned an economic value and traded for goods and services and ultimately conceptualized as a commodity.[25] In this view, privacy is subject to the economic principles of cost-benefit analysis and trade-offs. Users may be willing to exchange personal information if they perceive the benefits as being greater than a potential risk. For instance, popularity and a vast user base of recommendation services like *Netflix* (movies) and *Shelfari* (books) demonstrate that users are willing to register and submit both their personal data and behavioral preferences in exchange for a tailored recommendation service. [26]

In contrast, a bigger focus on privacy risk, defined as the degree to which an individual believes that a potential for loss is associated with the release of personal information to an entity, negatively impacts individual's intention to disclose personal information. [27] Perceived consequences of the disclosure of personal information, and thus the intention to disclose, becomes reflective of one's perception that potential benefits may be greater or lesser than possible negative outcomes. In order to reduce their concerns about disclosing personal information, individuals may employ various types of risk handling behavior.

---

[25] See, e.g., Posner, R.A., *An Economic Theory of Privacy*, AEI Journal on Government and Society, 19-26 (May/June 1978); Lessig, L., *Code is Law: On Liberty in Cyberspace* (2000), *available at*: http://harvardmagazine.com/2000/01/code-is-law-html (Professor Lessig embraces the vision of privacy as property suitable as a commodity to be traded).

[26] Such sharing and access to personal data, of course, represents a huge value to a service provider too. *See, e.g.*, Dylan Love, *Netflix's Recommendation Engine Drives 75% Of Viewership*, Business Insider, Apr. 9, 2012, *available at* http://www.businessinsider.com/netflixs-recommendation-engine-drives-75-of-viewership-2012-4 (highlighting how Netflix recommendation service, based on users activity and rankings, drives 75% of viewership).

[27] *See, e.g.*, Featherman, M., *Predicting E-Services Adoption: A Perceived Risk Facets Perspective*, International Journal of Human-Computer Studies, vol. 59, pp. 51-474 (2003).

E. Privacy paradox

Users' attitudes and risk sensitivity may not always correlate with their actual behavior (a phenomenon is known as privacy paradox). While expressed concerns about their personal information could be expected to drive one's intended and actual disclosure, several studies observed that in actual marketplace behavior "people are less than selective and often cavalier in the protection of their own data profiles."[28]

Acquisti and Grossklags observed this dichotomy and suggested that, "because of uncertainties, complexities, and psychological nuances <…>, many genuinely privacy sensitive individuals may decide against protecting their own personal information. The decision process considered by an individual therefore does not reduce to (just) an issue of different privacy sensitivities."[29]

Factors that also influence the user's privacy related choices include: limited information (including limited information about benefits and costs), bounded rationality, ideology, and market behavior. If the perception of these factors during an experiment or survey is different from their perception when an actual decision has to be taken, these factors may also cause the dichotomy between abstractly stated attitudes and actual behavior.[30] This presents one of the limitations of this study, since people may think of their intention, rather than actual behavior, when asked a research question, e.g., *Which of the following actions would you take to protect your privacy online?*

Norberg et al. demonstrated that the level of *actual disclosure* may significantly exceed an individual's *intention to disclose*; suggesting that in the realm of privacy, behavioral

[28] Patricia A. Norberg, Daniel R. Horne, and David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, Journal of Consumer Affairs, 41: 100–126, 101 (2007).
[29] Alessandro Acquisti & Jens Grossklags, *Privacy attitudes and privacy behavior*, Economics of information security 7 (2004), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti_grossklags_eis_refs.pdf.
[30] *Id.* at 7

intentions may not be an accurate predictor of actual behavior. Therefore, other explanations should be sought. They also found support to conclude that risk could significantly influences an individual's *intentions* to disclose, but neither risk nor trust were found to influence the *actual behavior* of users.[31]

Moloney and Poti found trust to have negative and significant influence on the intention, concluding that the more importance an individual places on the need to trust online third parties when disclosing personal information, the less inclined they are to impart information.[32]

Other than perception of risk, trust, and public opinion, can it be expected that the frequency of Internet use, as a display of trust in the Internet developed over time, also has an indirect effect on privacy related choices, *e.g.*, if more frequent users demonstrate a lower level of concern and, as a result, a different pattern of behavior? Thus, I will test:

Hypothesis 2: *Participants with more Internet experience will exhibit lower levels of concern about the privacy*

F. Privacy regulation models

While web services and online applications claim the right to use personal data and information technology to improve efficiency,[33] consumers exhibit the desire to control the flow and dissemination of their personal information.[34] Since policymakers consider privacy an individual right, they try to balance consumer interest in privacy against other competing

[31] Norberg et al., *supra* at 118.
[32] Moloney & Poti, *supra* at 61.
[33] Back in March 2012 Google reduced more than 60 privacy policies for all its products (e.g., Search, YouTube, Gmail, Calendar), down to one main "simplified" easy-to-read policy, while moving toward creating "one beautifully simple, intuitive user experience across Google". The company explained its reasons as follows: *"The main change is for users with Google Accounts. Our new Privacy Policy makes clear that, if you're signed in, we may combine information you've provided from one service with information from other services. In short, we'll treat you as a single user across all our products, which will mean a simpler, more intuitive Google experience." available at* http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html.
[34] Take targeted advertising as an example. Here, Internet companies argue they have the right to conduct business, but consumers and privacy advocates claim the right to be free of unwanted solicitations.

interests when adopting one of the regulation models. It's not only the balance of different group interests, however, that affects the model of privacy regulation - the level of users' concern also plays a role. Milberg et al. demonstrated that a rising level of privacy concern demands additional legal intervention,[35] thus leading to a stricter government model. Three privacy regulation models are often discussed that toggle between competing trade-offs and the various levels of government involvement:

Government regulation. Under this model, a government takes a paternalistic approach to protecting users as a weaker side in their dealings with private firms, and enacts privacy regulations with various levels of detail that dictate their behavior. Proponents of this model argue that the desire for profits, coupled with the economic value of personal information, will inevitably lead private firms to collect a great deal of personal information online while keeping users exposed to privacy risks.[36]

Self – regulation. Here, business representatives define and enforce standards for their sector with little or no government involvement.[37] It is assumed that users are aware of the potential privacy risks and can decide for themselves which of the data collection and processing practices they consider acceptable. The advocates of this approach argue that individual Internet businesses will enhance their competitive positions by responding to customer preferences for greater privacy, thereby leading to a more privacy friendly Web.[38] In addition, industry members

[35] Milberg et al. (2000), *supra* at 42.
[36] Dennis Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?* Seattle University Law Review, Vol. 34, No. 2, 2011. *Available at* SSRN: http://ssrn.com/abstract=1758078
[37] *Id.* at 31.
[38] See Eric Schmidt's written testimony to Congress, Sept 21, 2011 *available at* http://www.cnet.com/news/eric-schmidts-written-testimony-to-congress/ (In his testimony to a Senate panel looking into Google's growing dominance, Eric Schmidt, Executive Chairman of Google Inc., reiterated that competition was "just one click away" for the search engine company to counter accusations of being too dominant in the search engine market. Good example of such competition could be a search engine www.duckduckgo.com that presents anonymity as its competitive advantage ("The search engine that doesn't track you"). Its traffic has more than doubled since the revelations by Mr. Snowden. *See* Julia Angwin, *Has Privacy Become a Luxury Good?* N.Y. Times, Mar. 3, 2014, *available at* http://www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html?hp&rref=opinion&_r=1 Also, for a somewhat provoking description of how search engines may track their users see e.g. http://donttrack.us/).

will be more susceptible to accepting standards designed and imposed by their peers, rather than the government, and will spend less time and energy resisting them.[39]

Co-regulation. Under this model, an industry submits a code of conduct; the government authority then reviews it and advises on whether it is consistent with the national data protection law. It may also provide some assistance with its enforcement.[40] Privacy has been recognized as a fundamental human right by major international bodies of law, most importantly in Article 12 of the Universal Declaration of Human Rights,[41] Article 8 of the European Convention on Human Rights, [42] and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[43] Nearly every country in the world explicitly recognizes privacy rights in their constitutions. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. [44]

Russia, without a doubt, falls under a "government regulation" model. Given the breadth of the requirements imposed by the state in relation to the processing of personal data, I would go even further and characterize it is a "strict government model." As I demonstrate below, national privacy laws and complementing regulations are very detailed and require businesses to follow formalistic requirements. Failure to follow them can result in criminal, administrative, and/or civil liability.

[39] Hirsch, *supra* at 32.
[40] *Id.* at 52.
[41] The Universal Declaration of Human Rights, Dec. 10, 1948, http://www.un.org/en/documents/udhr/.
[42] The European Convention on Human Rights, Nov. 4, 1950, http://www.echr.coe.int/Documents/Convention_ENG.pdf.
[43] The Charter of Fundamental Rights of the European Union, Dec. 7, 2000, http://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[44] Article 23 of the Russian Constitution establishes the rights to the inviolability of private life, privacy of correspondence, personal and family secrets, the protection of honor and good name. Article 24 of the Constitution prohibits "the collection, keeping, use and dissemination of information about the private life of a person" without his or her consent. *available at* http://constitution.garant.ru/english/

G. Russian regulatory framework

On May 15, 2013, Russia ratified the "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data" that went into effect on September 1, 2013. The Convention establishes the right of all individuals to access, rectify, or erase their data when the information is not required for a specific purpose. It is the only legally binding international instrument in its field.

Russian Law on Personal Data No. 152 FZ dated 27 July 2006.[45] The law is similar in style to data protection laws in the European Union. It contains extensive restrictions on the collection, use, storage, transfer, and other processing of personal data. The law defines "personal data" to include any information related to a specific individual or to an individual who can be identified on the basis of such information. Examples of personal data include name, contact information, family, social and financial status, education, occupation, income, and other identifiable information. Operators of personal data may collect, use, store, or otherwise process personal data only for the specific purposes as defined by the law or with the subject's written consent, subject to detailed requirements on the content and form of the consent and the disclosures that must be provided to the consenting individual.

The law also contains many other requirements similar to the EU laws. For example, it requires operators to collect the minimum amount of personal data required to fulfill the purpose for which the information is collected, to ensure the integrity of the data, to minimize the storage of the data, and to implement appropriate data security measures. The law grants individuals and their representatives the right to access an individual's personal data and to object to the processing of the data. Russia's Federal Service for Supervision of Communications, Information

[45] Federal Law On Personal Data #152-FZ, *available at* http://www.consultant.ru/document/cons_doc_LAW_149747/.

Technology and Mass Media (Roscomnadzor) is the government agency tasked with overseeing compliance.

The law delegates the authority to issue complementing regulations regarding a number of issues to the government and responsible agencies. The authority to enforce the law's provisions and the power to issue penalties for violations is also delegated to these agencies. As an example of such regulations, the Russian Government has enacted Resolution No. 1119, dated 1 November 2012, which introduces measures and requirements in order to prevent any unauthorized access to personal data. There are also a number of other laws and regulations that regulate the protection of personal data in relation to specific areas of services or industries.[46]

H. The NSA scandal and recent legislative proposals

Russian state officials have been openly frustrated by a lack of authority over foreign Internet companies operating in Russia for a long time. The leaks by Mr. Snowden presented a unique opportunity to push for tighter controls over the Internet,[47] ostensibly in order for Russian users to safeguard their private information from spying. This debate and corresponding accusations resulted in the proposal of new legislative initiatives designed to strengthen the state's control over the use of personal data, with a stricter liability for its violation.

Legislative initiative 428884-6. The draft law targets individuals or legal entities, which enable the communication between users. The bill would mandate operators that are either incorporated in the Russian jurisdiction, or accessible by users located in the Russian

[46] As an example of a very detailed regulation, earlier in April 2014 the Russian Central Bank ordered local banks to take appropriate measures in order to toughen the regime of a storage and destruction of records containing personal data of their customers. Failure to do so was to entail the audit by the regulator. *See*, Anastasia Alekseevskih, *Regulyator potreboval ot bankov lusche hranit dannye klientov*, Apr. 8, 2014, *available at http://izvestia.ru/news/568804*.

[47] See, Andrew Kramer, *N.S.A. Leaks Revive Push in Russia to Control Net*, N.Y. Times, July 14, 2013, *available at* http://www.nytimes.com/2013/07/15/business/global/nsa-leaks-stir-plans-in-russia-to-control-net.html?_r=1& ("We need to quickly put these huge transnational companies like Google, Microsoft and Facebook under national controls," Ruslan Gattarov, a member of the upper chamber of the Russian Parliament (Federation Council), said in an interview. "This is the lesson Snowden taught us.")

jurisdiction, to "store all information about the arrival, transmission, delivery, and processing of voice data, written text, images, sounds, or other kinds of action" on Russian soil. Moreover, domestic and foreign website operators would have to inform regulators from the moment users in Russia start using their services. The draft also includes a vague jurisdictional clause claiming applicability to all websites that Russian users access: "In the event that the communication service organizer is located beyond the borders of the Russian Federation, but the user of the services is located within Russian territory, the location of services rendered is the territory."[48]

As mentioned above, the higher level of privacy concern among users normally demands a stricter government model. This study, however, will explore a different direction – whether a level of government involvement in a regulatory model affects who users tend to blame if their privacy is breached. Therefore, I state:

Hypothesis 3: *In a paternalistic (highly regulated) model, which Russia is, users tend to put more blame on the government or Internet businesses than on themselves in the case of privacy breaches*

I. Does age affect privacy attitude?

Despite a common belief that the younger online population is less concerned with maintaining privacy than older people simply because they share online more,[49] several studies demonstrate that the situation is more nuanced. Hoofnagle et al. showed that young people's attitudes did not differ much from older Americans on issues of information privacy[50]. Another study, sponsored by Microsoft, found that "[p]rivacy and security rank as college students' #1

[48] When I nearly finished this paper, the draft law was approved by the Parliament (with exception of the 'jurisdictional clause'), signed by the President on 05.05.2014, and will go into effect on August 1, 2014.
[49] *See, e.g.*, Ariel Maislos, chief executive of Pudding Media, quoted in Louise Story, *Company Will Monitor Phone Calls to Tailor Ads*, New York Times, Sept. 24, 2007, *available at*: http://www.nytimes.com/2007/09/24/business/media/24adcol.html.
[50] Chris Hoofnagle et al., *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* 3 (April 14, 2010), *available at*: http://ssrn.com/abstract=1589864.

concern about online activity."[51] Young adults may be more accepting of online companies trying to monetize their data than other age groups[52]; but at the same time, they are more skeptical about the government's implicit security-for-privacy bargain.[53] Solove suggested that the younger online population, despite having an attitude to share more online,[54] views privacy as a method to control information flow.[55] This study will compare various age groups with respect to attitudes toward online privacy protection and privacy-protecting behavior, and I submit the following hypothesis:

Hypothesis 4: *Younger Internet users in Russia demonstrate a different privacy risk attitude and behavioral pattern*

J. Previous studies on privacy attitude and behavior

Although the level of government involvement in the regulation of information privacy is associated with the country's level of privacy concern,[56] and Russian officials in their public statements claim that they, first and foremost, worry about Internet users and want to protect their interests, there is no sufficient empirical data on Russian users' attitude about their online privacy and their corresponding behavior. Occasionally, polling organizations in Russia have asked some questions related to privacy in their regular omnibuses. One such poll was conducted by the Fund Public Opinion in April 2013 with the following main results:[57]

---

[51] Anthony Salcito, *Privacy and security rank as college students' #1 concern about online activity, according to new poll*, Sep.25, 2012, *available at* http://blogs.technet.com/b/microsoft_in_education/archive/2012/09/25/privacy-and-security-rank-as-college-students-1-concern-about-online-activity-according-to-new-poll.aspx

[52] Drew Desilver, *Young Americans and privacy: 'It's complicated', available at* http://www.pewresearch.org/fact-tank/2013/06/20/young-americans-and-privacy-its-complicated/

[53] Pew Research Center, *Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic*, Jun. 10, 2013, *available at* http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/.

[54] Solove explains this phenomenon as follows: young people, especially teenagers, may not think through the consequences of their actions; new technologies have become a significant part of their lives, and the technologies make it very easy to share

[55] Daniel Solove, *Do Young People Care About Privacy?* Oct. 10, 2012, *available at* http://www.linkedin.com/today/post/article/20121010201716-2259773-do-young-people-care-about-privacy.

[56] Milberg et al. (2000), *supra*. Also, Colin J. Bennett, *Regulating privacy: Data protection and public policy in Europe and the United States* (1992).

[57] Fond Obschestvennoe Mnenie, *Zaschita Personalnyh Dannyh*, May 23, 2013, *available at* http://runet.fom.ru/SMI-i-internet/10922.

- Only 23% correctly named Roscomnadzor as the privacy watchdog;
- Top 3 privacy violations reported by respondents include unauthorized email and sms (27%), "cold calling" (23%), and hacking of social networks and distribution of personal data (9%);[58]
- 32% of respondents do not pay attention to privacy notices when filling out paper documents,[59] while 16% do not pay attention when submitting their information online;
- 68% believe that the protection of personal data is inadequate in Russia.

Another polling organization, Levada-Center, conducted a national survey in October 2013 and asked respondents how important they felt confidentiality was in regards to online activities and correspondence. The results were as follows:

- Very important / Rather important (58%);
- Not very important (12%);
- Not important at all (8%);
- Hard to tell (22%).[60]

While the results of these surveys may be useful to some extent in order to assess the development of the public's awareness over time, the scope of the surveys may not be sufficient for an in-depth data analysis, especially of the potential dichotomy between attitude and behavior. One should also be wary of a number of significant developments in the privacy environment in the last twelve months that could affect users' attitude towards the subject.

A large number of surveys on privacy attitude and awareness were conducted in other countries. These surveys can be grouped based on: specific industry practice, e.g. attitude

[58] Interesting that the top two "privacy" violations in this study involve spam and cold calling, which are about intrusion on the person, not about use of data.
[59] The number may be even higher than 32% as people bias their answers to give answers they think are desirable.
[60] Levada-Center, *Tseli i konfidentsialnost rossiyan v Internete*, Nov. 11, 2013, *available at* http://www.levada.ru/11-11-2013/tseli-i-konfidentsialnost-rossiyan-v-internete.

regarding targeted advertising, [61] specific online services,[62] demographics (e.g. difference in privacy attitude between younger and older generations),[63] or a country.[64]

3. METHODOLOGY

A. Data collection

The Fund Public Opinion (*Fond Obschestvennoe Mnenie*) was commissioned to include the survey questions in one of its omnibuses (biweekly national polls) that were conducted in December 2013, with a nationally representative sample of 3000 adults. Because of the limitations on the maximum number of questions, they were divided into two groups, with a different set of privacy related questions in each group. Similar demographic questions on age, education, place of residence, material status,[65] and the Internet use were used, with 1500 respondents in each group.

To ensure a random sampling, interviewers followed their standard sampling procedures (e.g. establishing general criteria for selecting a street, house and apartment, establishing minimum and maximum representations by gender, location, age group, education, and limiting the maximum number of interviewees on a single "route").

Among the respondents from both groups that completed the survey, 1620 (54%) were grouped into an "Internet users" category, meaning they identified themselves as having used the

[61] Aleecia M. McDonald & Lorrie F. Cranor, *Americans' Attitudes About Internet Behavioral Advertising Practices*, in *Proceedings of the 9th Workshop on Privacy in the Electronic Society (WPES)* (Oct. 4, 2010).
[62] *See, e.g.*, Bernhard Debatin et al., *Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequence*, Journal of Computer-Mediated Communication 15, 83-108 (2009).
[63] Chris J. Hoofnagle et al., *supra*.
[64] Office of the Australian Information Commissioner, *OAIC Community Attitudes to Privacy survey Research Report* (2013), available at http://www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013
[65] "Material status" is a category that identifies respondents' financial position in terms of income and assets. The category was broken down into following levels: "No enough money even for a food" ("Level 1"), "Enough money for a food, but can't afford clothes and shoes" ("Level 2"), "Enough money for clothes, shoes, but can't afford home appliance" ("Level 3"), "Enough money for home appliances, but can't afford a car" ("Level 4"), "Enough money for a car, but can't afford a house or an apartment" ("Level 5"), "Enough money to buy a house or an apartment" ("Level 6").

Internet in the last day, week, or month.[66] Such level of the Internet use is in line with earlier reports by the Fund on the number of monthly Internet users in Russia.[67]

B. Data analysis

Data analysis from the survey results included cross-tabulation and significance testing (regression). The results were tested for statistical significance and, unless otherwise noted, only the ones with a confidence level greater than 99% were reported (*i.e.,* a p-value of less than .01).[68]

Cross-tabulation is a statistical process that summarizes categorical data to create a contingency table. It allows researchers to see patterns of response, determine whether there are any different responses between variables, and decide whether variables are dependent on others. For example, the results of this survey demonstrate that there is a clear relationship between the age of respondents and their view on whether a social network is a public or private space.

In addition to descriptive statistics and bivariate comparisons of individual variables the results were also checked using regression (linear and logistic) to determine the effect of which variables remained significant after accounting for interactions (correlations) among the variables within each set. Regression analysis is a class of statistical model used to describe or estimate casual relationships among dependent variables and one or several independent variables. Although statistical data may not always be sufficient to convey the flavor of all interactions, they may often help explain the prevalence and character of some.

---

[66] Thus the sample size was limited to 839 respondents in one group, and 781 in another, with a confidence level 95%, and confidence interval 3.38 and 3.51 respectively.

[67] See, e.g., Fund Public Opinion, *Internet v Rossii: dinamika proniknoveniya. Osen' 2013*, Jan. 14, 2014, *available at* http://fom.ru/SMI-i-internet/11288.

[68] In some interesting cases I also report those results that have a *p* value between .01 and .05

C. Limitations

The results of the study should be read within its limitations. First, the level of privacy concerns is very likely to be influenced by external sources of information (*e.g.*, the media) that report negative practices associated with privacy, and more specifically, the risks apparent in personal information access and availability. The issue of privacy was often in the news in Russia in 2013, and public debate triggered by the NSA scandal may have had some effect on how people chose to respond to some of the survey questions, in particular, questions on general attitudes to privacy and trust.

Second, because of the technical limitations, the survey questions were divided into two groups. Although demographic data were similar for both groups of respondents, the responses to the questions could be analyzed and cross-correlated only within the same group. As a result, there were fewer opportunities to explore correlations between the responses.

Third, as mentioned above, earlier surveys conducted in Russia offer very limited opportunity to compare the responses over time in order to observe the trends in the change of attitude and behavior.

4. SUMMARY OF THE FINDINGS

In addition to the four hypotheses mentioned above, my primary goal was to obtain a baseline understanding of how Russian Internet users evaluate online privacy based on four aspects: attitude, awareness, behavior, and trust.

Awareness. The users are generally aware of the data collection and targeted advertising practices: 59% believe that most or all websites and smartphone applications collect information about the users who visit or use them, and 51% notice advertising that is targeted at them based on their search queries and any other online activity. There is no evidence that the age of the

respondents contributed to the level of awareness but frequency of the Internet use and the level of education demonstrated some relationship.

Attitude. Russian users are nearly equally divided on whether or not they feel worried about the confidentiality of their personal data online. Material status has a significant effect on users' level of privacy concern. When it comes to privacy risks, users are most worried about the risks to their financial data. Almost one-third of the users also feel annoyed with unsolicited advertising. Interestingly, the secret access to their data by law enforcement is of concern only to 11% of users.

Behavior. It is a troublesome finding that more than a half of the respondents (53%) say that they would not take any preemptive action to protect their privacy. More privacy-conscious users, (21%), indicated that they would choose not to use a web site, smartphone app, or online service because of the information requested. In case of a privacy violation, almost a third of users (30%) would not file a complaint. Material status, frequency of the Internet use, and age have a significant effect on the likelihood to take some protective measures, suggesting that younger users are more likely to take measures to protect privacy.

Trust. Respondents did not demonstrate any strong preference or trust in either online or offline environments, as well as Russian or foreign online resources when it comes to the protection of their privacy. 21% of users believe that both Russian and foreign resources equally protect their personal data, with every sixth user (16%) demonstrating equal preference for either Russian or foreign resources.

5. DETAILED ANALYSIS

In Table 1 (Appendix 1) the characteristics of the Internet users are presented as an average based on the demographics of the two groups of respondents. Between Internet users and non-Internet users,[69] differences in occupation ($p < .001$) and age ($p < .001$) are observed,[70]

but no difference in gender (p=.159) is present. Internet users also tend to have a higher material status, live in more populous locations, and have higher level of education (all $p < .001$).

A. Awareness

Awareness was assessed on two aspects: knowledge of the passive collection of personal data and knowledge about targeted advertising.

Knowledge of the passive collection of personal data.

Users were asked to estimate the proportion of websites and smartphone applications (or apps) that collect personal information. As Chart 1 shows, almost a third of Internet users (31%) believe that all or almost all web sites / applications passively collect information about their users, and 28% believe that most of them do so. Only 2% think that none, or only a few, collect such data.

[69] I define "non-Internet users" for the purpose of this comparison as those who provided one of the following responses to the question "Have you ever used the Internet": "Never used", "In the last 3 months", "In the last 6 months", or "In the last year".
[70] Internet users are younger: mean age 35.3, std. dev 12.7, as compared to non-users' mean age 57.0, std. dev. 15.3; t(2685.78)=41.817

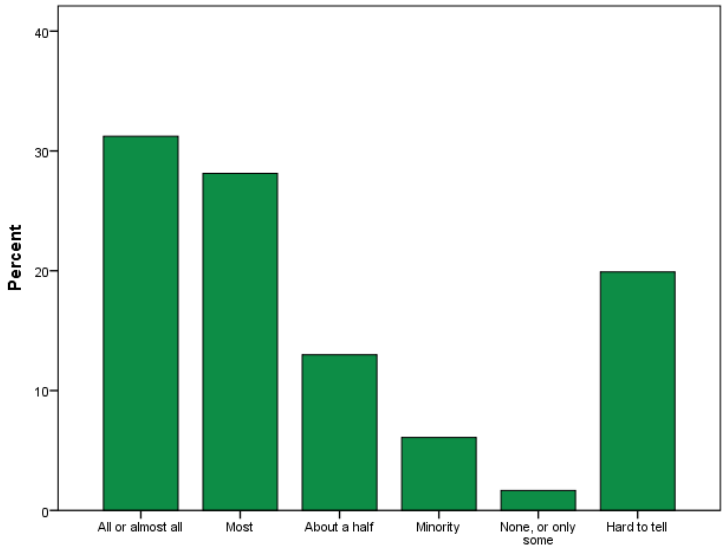

Chart 1. *What proportion of websites/smartphone apps do you think collect information about the people who visit/use them? (One response)*

Both the age (p = .516) and frequency of Internet use (p = .843) were unrelated to the response to this question. There is no significant relationship between a better awareness of passive data collection and propensity to complain in case of privacy breach, except that those who gave "Hard to tell" response (that could signal a lack of knowledge) are also likely to choose not to complain.[71]

Those users who think that fewer of web-sites / apps collect personal data are more likely to ask organizations why a particular piece of information is being collected.[72]

20% users who gave "Hard to tell" response tend to be less frequent Internet users.[73] This may provide some limited support to those who advocate for more privacy and Internet educational campaigns, rather than a strict government regulation model that would help users make informed decisions as to the protection of their privacy online.

[71] See Table 2.1 in Appendix 2.
[72] N = 672; rho = .106; p = .006
[73] See Table 2.2 in Appendix 2.

Knowledge about targeted advertising.

Targeted advertising is the practice of collecting data about an individual's online activities for use in selecting which advertisement to display. Targeted advertising creates profiles for Internet users based on a variety of different data types and inferences drawn from those data.[74]

Respondents were asked if they notice advertising that is targeted at them and that takes into an account their search queries and any other online activity, and how they felt about such advertising. 44% of the users don't notice this practice online. A third of Internet users (32%) are generally uncomfortable with the prospect of information being captured and used to target advertising to them. Nonetheless, 19% of the respondents are rather comfortable with such advertising.

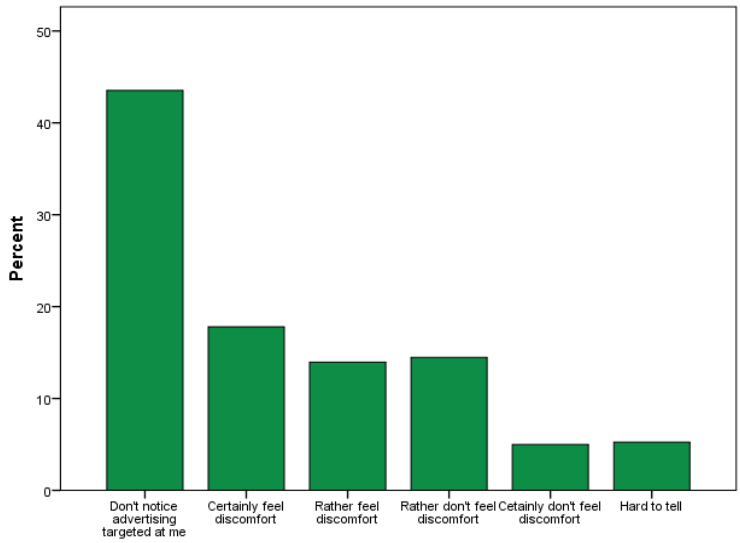

Chart 2. *At the moment many web sites use targeted advertising, based on the user's activity online, i.e. his search queries, visited sites, email content, etc. Do you or do you not notice advertising that is targeted at you, that takes into an account your search?*

[74] For explanation of how targeted advertising works, *see, e.g.*, Clint Pumphrey, *How do advertisers show me custom ads? available at* http://computer.howstuffworks.com/advertiser-custom-ads.htm.

Trends were apparent in respondents who notice targeted ads. These users were more likely use Gmail ($p = .017$),[75] the Opera browser ($p < .001$), the Chrome browser ($p < .001$), Twitter ($p = .004$), and Facebook ($p < .001$). There was no significant difference between those who notice and those who don't on age ($p = .629$), but more frequent Internet users and users with a higher level of education are more likely to notice targeted ads.[76]

B. Attitude

I sought to assess Internet users' attitudes by asking respondents:

- Which of their data cannot be used without their permission?
- Which of the actions may cause the biggest threat to their privacy?
- Do they feel worried about the protection of their privacy?
- How do they perceive social networks (as private or public space)?
- How do they feel about targeted advertising?

Most valued personal data.

Users generally do not want to see any of their data to be used without their permission, valuing such things as passport number, email content, and pictures the most.

[75] The finding that Gmail users are more likely to notice targeted ads is also in line with the findings from the study of the awareness of online behavioral advertising in the USA. *See, e.g.,* Aleecia M. McDonald & Lorrie Faith Cranor, *An empirical study of how people perceive online behavioral advertising*. Tech. Rep. CyLab Technical Report 09-015 (Nov. 2009), *available at* https://www.cylab.cmu.edu/research/techreports/2009/tr_cylab09015.html.
[76] See Table 2.3 in Appendix 2.

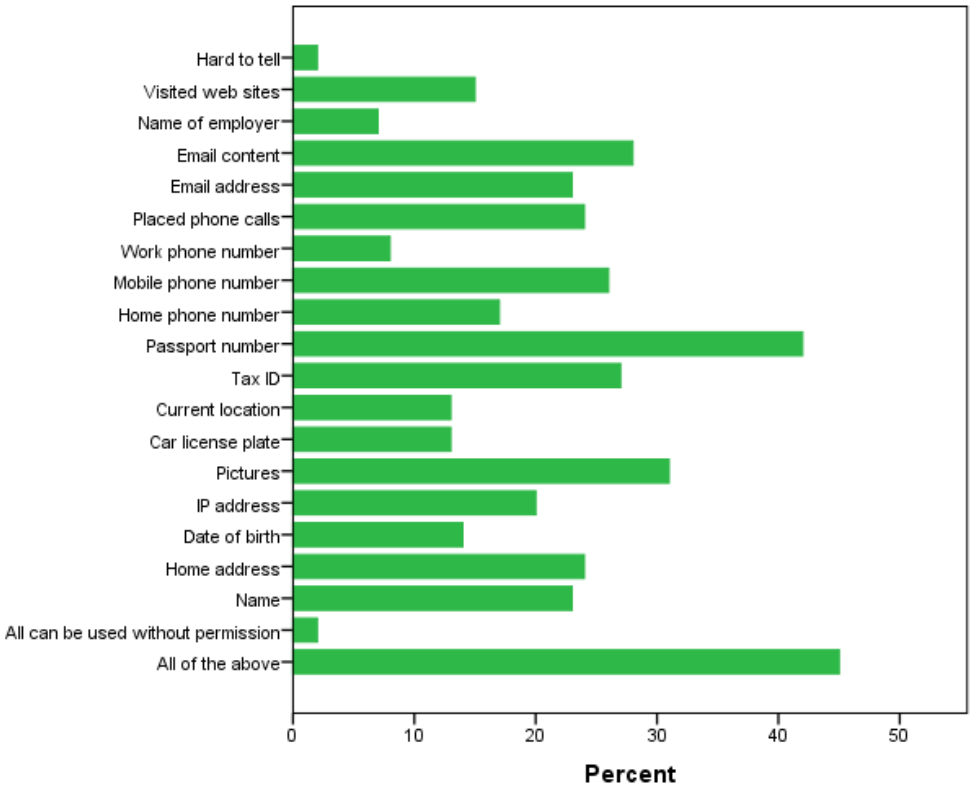

Chart 3. *Which of the following data cannot be used without your permission*?

Biggest harm.

When asked about what actions may cause the biggest threat, of primary concern to respondents were incidents that lead to direct monetary losses: credit card fraud (59%), fraud with electronic payment systems, and/or sms payments (36%). Such monetary concern was related to a higher level of education and occupation (for both $p < .001$), but was unrelated to material status of respondents ($p = .045$).[77] The NSA scandal did not generate a meaningful debate about the Russian government surveillance practices, and possibly because of that, only a small number of people was worried about law enforcement authorities having secret access to their personal information (11 %). Those who indicated this was a potential threat did not

[77] Would be significant at the 95% significance level

demonstrate strong preference for Russian or foreign resources when asked about which better protected their data (p = .793).

The transfer of personal data abroad is of concern to one tenth of the respondents. Interestingly, attitude about whether Russian or foreign resources better protect data does not significantly affect such opinions (p = .283). In addition, almost a third (29%) are worried about the unauthorized use of personal information for marketing purposes.

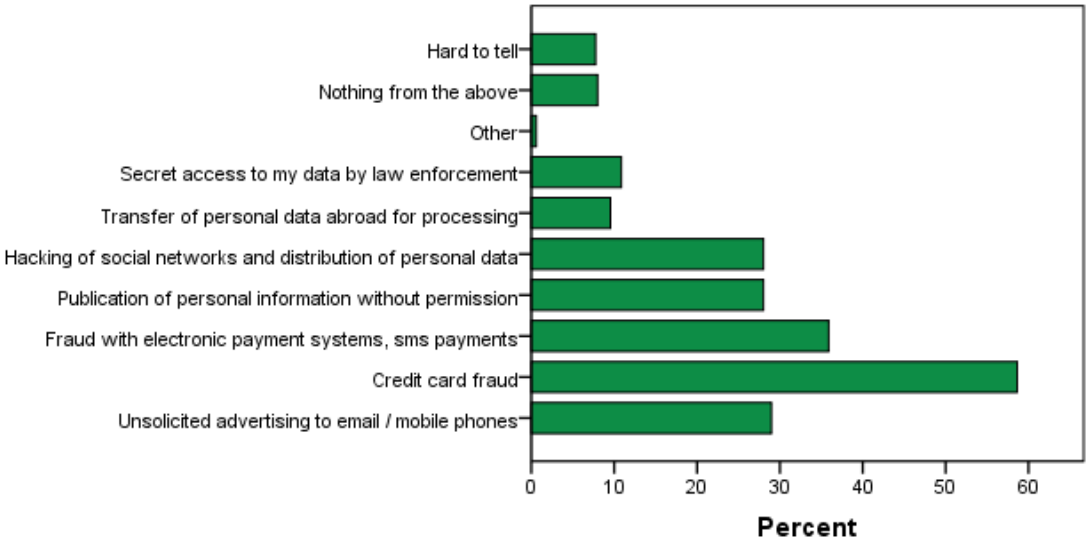

Chart 4. *Which of the following do you believe may cause the biggest threat to people like you?*

Feeling of worry about confidentiality online.

Users were divided equally on whether they feel worried or not about the confidentiality of their personal data online.

Looking into potential factors that may affect this attitude, while controlling for age, and frequency of the Internet use, material status has the strongest (negative) effect on the feeling of worry, while a higher level of education contributes to increased worry.[78] Getting richer helps take the worry away. Neither frequency of Internet use, nor the age of respondents has a

[78] See Table 2.4 in Appendix 2.

significant effect on the feeling of worry. Respondents who feel more worried reported that they also became more worried over the last year ($p < .001$).[79]

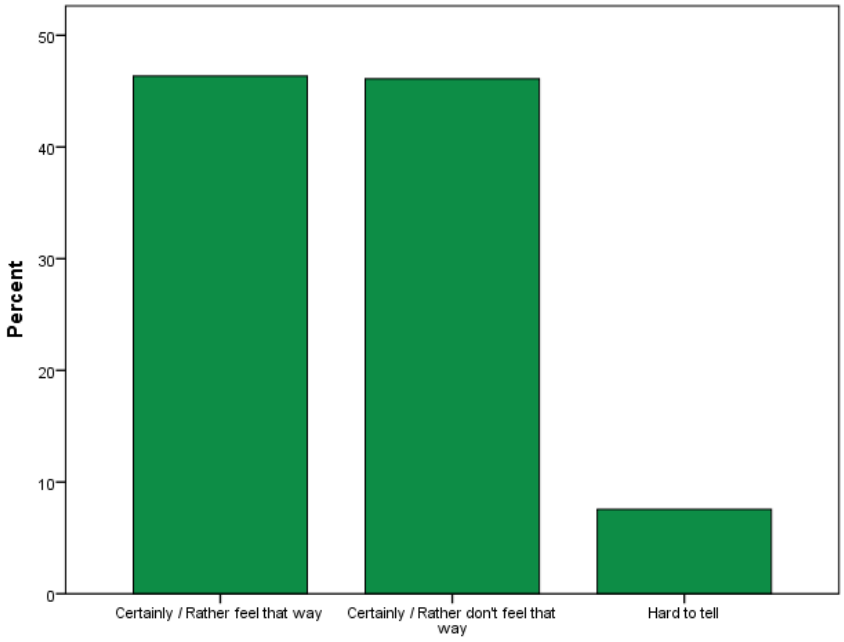

Chart 5. *Overall, do you feel worried about confidentiality of your personal data online?*

Social networks: private or public space?

The majority (56%) believes that social networking is mainly a private space, where information is shared with relatives and friends. However, 26% of the respondents, among which younger respondents prevail, believe it is a public space where information is shared with all users of the social network.[80]

[79] N = 670; rho = .479; p < .001
[80] See more on the effect of age in the Chapter "Hypotheses testing"

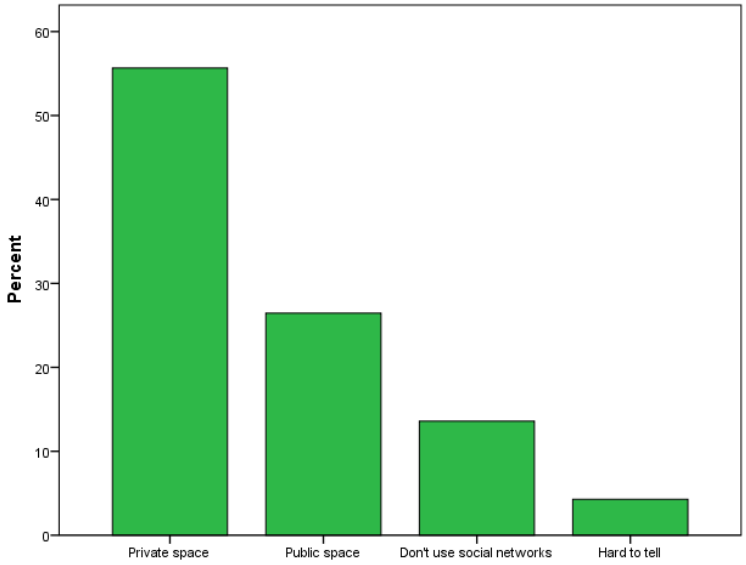

Chart 6. *If you use social networks, is this a private space where you share information with your relatives and friends, or a public space where you share information with all users of this social network?*

In bivariate correlation gender appears to have a significant effect on this attitude (p = 0.01), suggesting that female users are more likely to view social network as private space where they share information only with their friends and family members; while male users think of it more like a public space.

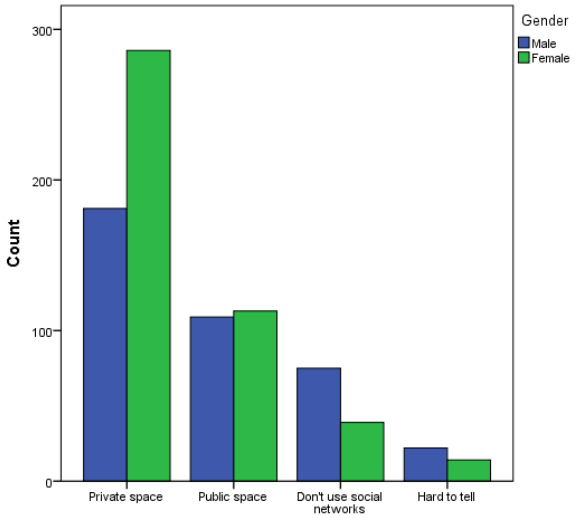

Chart 6.1 *Social networks: private or public space? (by gender).*

When controlling for all demographic and socio-economic factors (education, gender, material status, and frequency of the Internet use), age (p = .035) appears to have certain level of significance, suggesting that older users tend to view social network as private space.[81]

I was also interested in understanding whether or not an attitude towards social networks (private vs. public space) is then exhibited through users' behavior to protect their privacy. Are those who think that social network is a private space taking measures to protect their data? A bivariate comparison shows no difference between those who believe social networks are a private or public space in regards to privacy behaviors, including the likelihood of adjusting privacy settings on social networking sites (p = .573).

This information was further analyzed to determine if those respondents who view social networks as a private space were more likely to complain to the authorities in case of their privacy breach (response to the question *"If your privacy were breached, would you complain, and if yes - to whom?*") and found no significant likelihood. This may be indicative of a potential privacy paradox – a mismatch between an attitude (social network is a private space) and demonstrated behavior (protecting information from others by adjusting privacy settings), and may have some policy implications. It provides an evidence to assert that making people more aware of the fact that their information may be exposed to public does not necessarily lead to them taking actions to protect it.

Feelings about targeted advertising.

32% of the users surveyed are uncomfortable with the prospect of information being captured and used to target advertising and other offerings to them. Nonetheless, 19% of the online public doesn't feel discomfort with targeted advertising based on their Internet behavior.

[81] Would be significant at the 95% significance level. See Table 2.5 in Appendix 2.

In fact, there was no difference between those who did or didn't feel discomfort in terms of frequency of Internet use (p = .037).[82] Those who do feel discomfort about targeted advertising are more concerned with the use of their search queries (p < .001), visited sites (p < .001), email content (p = .009) and information from social networks (p = .004). Interestingly, users of Gmail are more likely to say no to the targeting based on their email content (p = .019),[83] but other than this, there was no significant effect of Gmail use on the overall feeling of discomfort with respect to targeted advertising (p = .49). Those who notice targeted advertising are also more likely to not want their current location to be used for this purpose (p = .011).

C. Behavior

Behavior was assessed based on users' willingness to complain in case of privacy breach and which measures they said they would take in order to protect their privacy.

30% said that they would not complain. A trend showed that those users were also more likely to give a "Hard to tell" answer, demonstrating a lack of strong opinion when asked about what actions they would take to protect their privacy (p = .019). These respondents, however, were no more likely to answer "Hard to tell' to the other questions. Those who would decide to complain would submit either to an organization that is in possession of their personal data (18%), a court (18%) or Russian Privacy Watchdog - Roscomnadzor (15%).[84]

In comparing the two groups -- those who would and would not complain -- no difference was determined on either on the respondent's awareness of passive collection of personal information, nor in who they would blame. Two statistical trends, however, indicated that higher

[82] Would be significant at the 95% significance level

[83] Gmail is well known for indexing email content for the purpose of showing to its users targeted ads. For the description see, *e.g.*, https://support.google.com/mail/answer/6603?hl=en.

[84] Based on the Roscomnadzor's annual reports, we see a significant upward trend in the number of actual submissions from users indicating a rise in users' awareness and their willingness to complain: 1829 submissions in 2010, 3920 – in 2011, 5368 – in 2012, and 10007 – in 2013. *Available at* http://rkn.gov.ru/personal-data/reports/

material status (p = .019),[85] and education (p = .012)[86] were related to a greater likelihood of complaining. Other demographic factors were unrelated, including, gender (p = .078), age (p = .767), place of residence (p = .652), and occupation (p = .313). There was also no relationship between likelihood to complain and frequency of the Internet use (p = .275), as well as believing social networks are public or private spaces (p = .276).

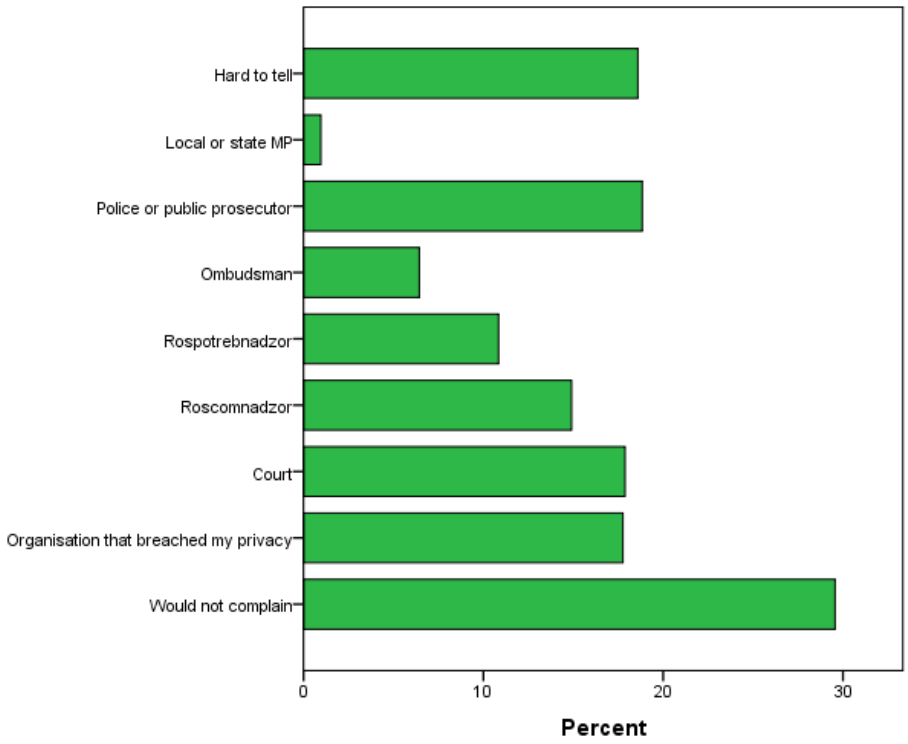

Chart 7. *If your privacy were breached, would you complain, and if yes - to whom?*

Measures taken to protect privacy.

The results paint a bleak picture of users' privacy cautious behavior (or a lack of it). 53% of the Internet users indicated that they would do nothing to protect their privacy online. This group was also likely not to complain in case of the privacy breach. Those who said they would do nothing were less concerned about credit card fraud, electronic and sms payment fraud, and

[85] Would be significant at the 95% significance level
[86] Would be significant at the 95% significance level

hacking of social networks (all $p < .001$), and were more likely to state that none of the mentioned potential threats bothered them ($p < .001$). This suggests a rational choice as these users select a behavior model that is aligned with their beliefs. Users who selected one or more of the actions to protect their privacy were also more likely to complain in the event of a privacy breach ($p < .001$). Almost 22% of respondents would select not to use a web site or app in case of concerns about the scope of the requested information. This group demonstrates an example of "privacy calculus" in action. Among demographic and socioeconomic factors, people with a higher material status are more likely to choose this option in order to avoid privacy risks.[87]

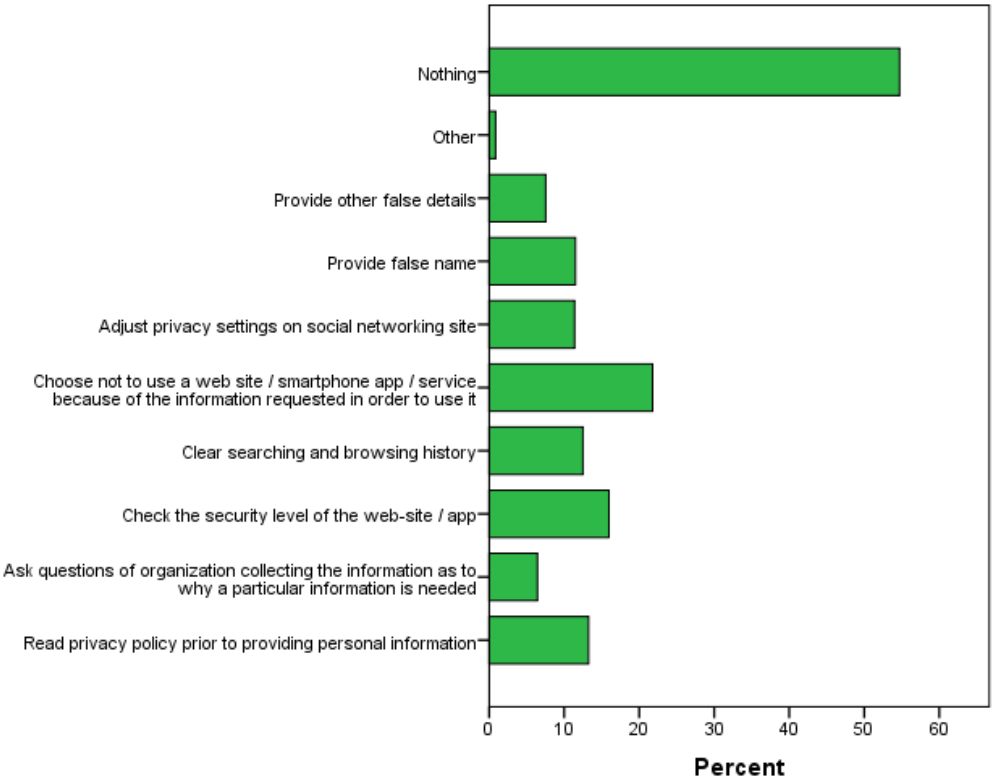

Chart 8. *What of the following actions you would have to take to protect your privacy online?*

Frequency of Internet use and age also contribute to the propensity for taking protection measures, suggesting that younger users are more likely to take certain actions to protect their data (*e.g.*, adjust privacy settings on social network, or check the security of the web site).[88]

[87] See Table 2.6 in Appendix 2.
[88] See Table 2.7 in Appendix 2.

D. Trust

This section examines the users' privacy preferences in online and offline environments, as well as local and foreign online resources.

Online vs. Offline.

Users do not demonstrate a very strong preference in terms of trust in regards to online vs. offline environments. They either have difficulty expressing their preference (41%), or think that personal data is protected equally bad (31%), or equally well (10%) both online and offline. None of the noteworthy factors (education, age, frequency of the Internet use, gender, level of worry about confidentiality online) showed any significance. In addition, none of the demographics factors show a significant effect on the preference.

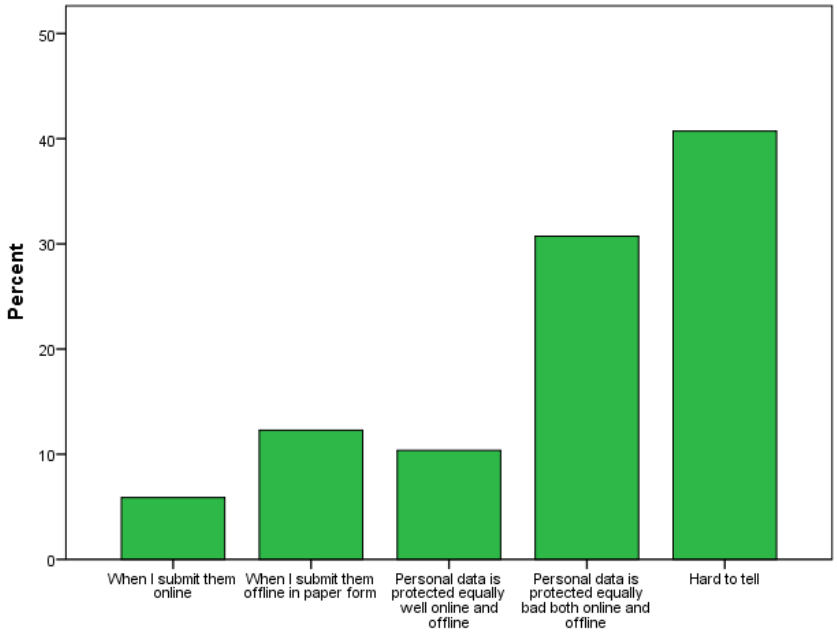

Chart 9. *In which case do you think your personal data is better protected?*

Local vs. Foreign.

Users do not demonstrate a prevailing trust in either foreign or local Internet services. 21% of users think that Russian and foreign resources are equally protecting their personal data, with an equal divide of preference (16%). Similarly, no demographic factors were shown to be significant regarding preference for online vs. offline.

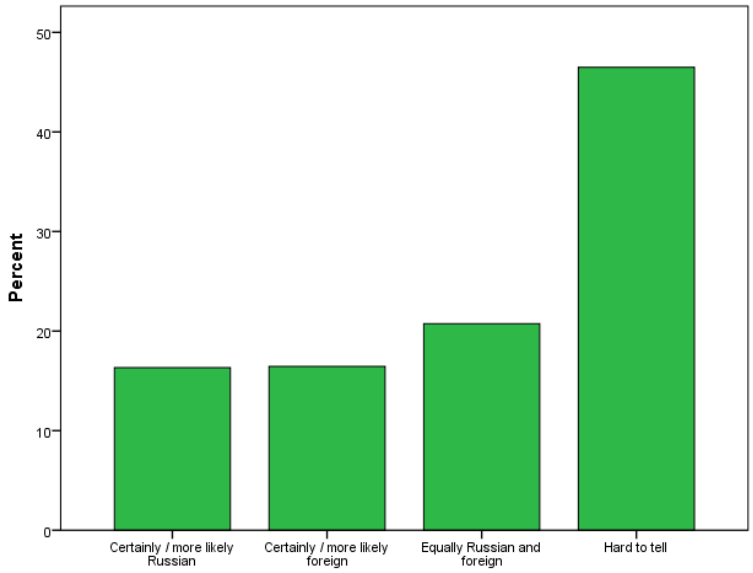

Chart 10. *Which resources (web-sites, applications) do a better job at protecting personal data of their users: Russian or foreign?*

Trustful resources.

When asked about which of the resources do a better job at protecting privacy, users clearly demonstrated more trust in local social networks compare to foreign: Facebook (2%) and Twitter (1%) vs. Vkontakte (9%) and Odnoklassniki (10%). This could be an effect of the media coverage of the NSA scandal, which often associated the leaks with Google, Facebook, and other US companies. Understandably, the trust in these products is strongly correlated with their use (for all pairs $p < .001$).

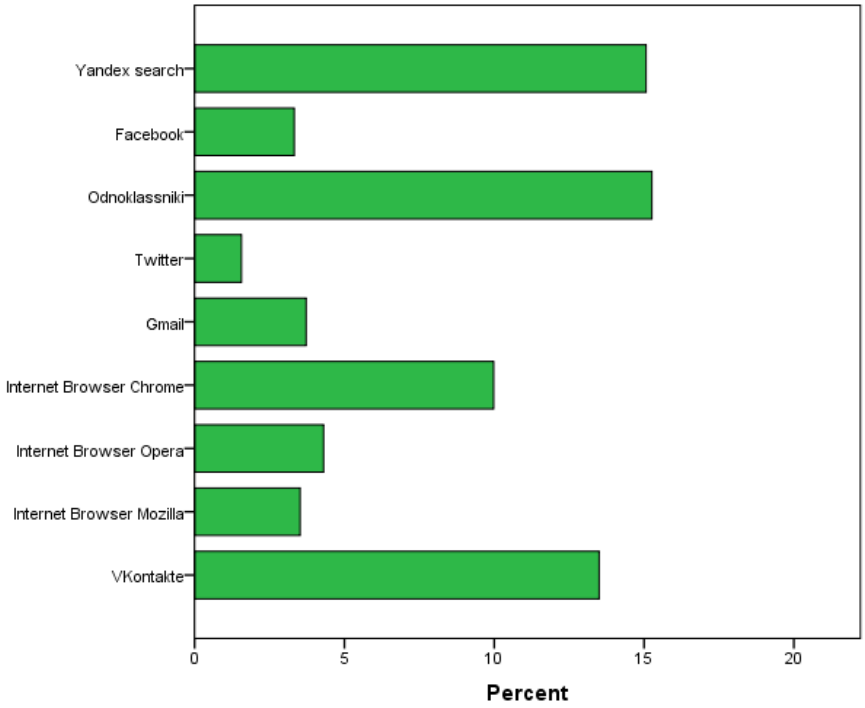

Chart 11. *Which of the following resources do you think do a better job at protecting confidentiality of personal information?*

E. Hypothesis testing

H1: NSA / Snowden scandal last year significantly affected users' attitude (HOLDS)

I attempted to estimate the effect of the NSA/Snowden scandal on user's privacy concern, and asked users if they became more or less worried in the last year about confidentiality of their personal data, or felt the same. 22% of respondents reported that they have become more worried.

This is a significant jump and can at least partially be attributed to the massive media coverage of the NSA scandal in Russia in 2013. Still, 68% of the users reported that they feel the same way as they did a year ago, with some saying they feel even less worried (2%).

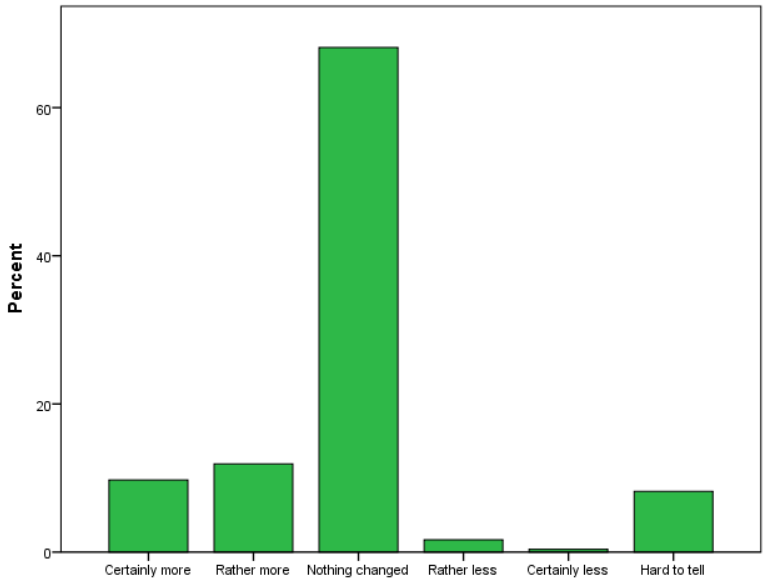

Chart 12. *In the last year were you worried more or less about the confidentiality of your personal data, or the same?*

There is a significant relationship between the overall feeling of worry about the confidentiality of online personal data and the increase of that worry in the last year – people who in general feel more worried have also likely become more worried.[89] Similarly to the effect on the overall feeling of worry, a higher material status contributed to less worry in the last year as well.

H2. Participants with more Internet experience will exhibit lower levels of concern about their privacy, and different privacy behavior (PARTIALLY HOLDS).

The effect of the frequency of Internet use was tested against the responses within the categories of "Awareness," "Attitude," and "Behavior." It was determined that the frequency of Internet use had no effect on the overall feeling of worry about confidentiality online (neither generally, nor in the last year). More frequent users, however, do demonstrate a different privacy behavior on some aspects. They are more likely to apply some measures to protect their privacy,

[89] N=686, B=.375, t=4,444, p < .001

including, checking the security of a web-site before submitting personal information,[90] adjusting privacy settings on social networks,[91] or providing false name.[92] They are also less likely to indicate that they would do nothing to protect their privacy.[93]

More frequent users show a tendency to choose to complain to Roscomnadzor, which is the most appropriate authority among the presented choices, if they believe that their privacy is breached.[94]

Thus, the hypothesis holds partially true in respect to behavior, and does not hold in respect to the level of concern.

H3: In a paternalistic (highly regulated) model, users tend to put more blame on the government or Internet businesses, than on themselves, in case of privacy breaches (HOLDS)

Users are more inclined to blame the government (29%) or a web-site / app owner (31%), and less to blame themselves (19%) for breach of privacy.

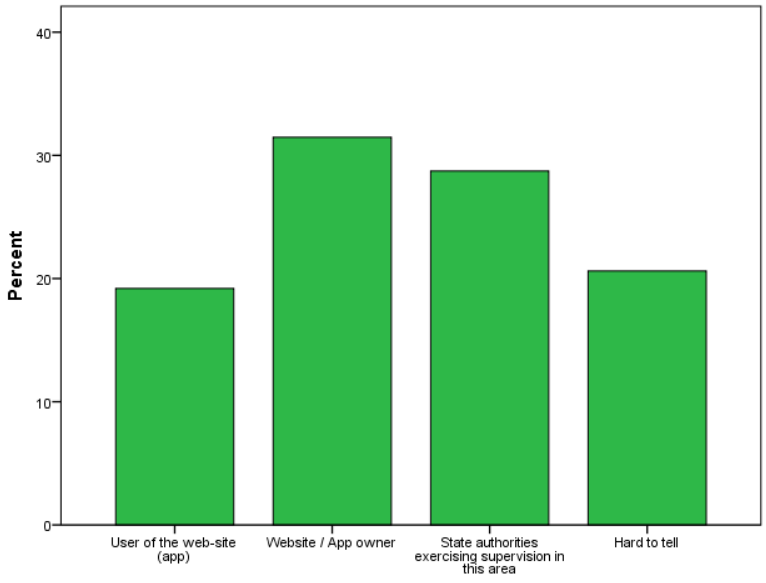

Chart 13. *Who do you think is often to blame for breach of privacy?*

[90] N = 839, p = .005, rho = .098
[91] N = 839, p < .001, rho = .122
[92] N = 839, p = .003, rho = .102
[93] N = 839, p = .002, rho = -.106
[94] N = 839, p = .011, rho = .087

In a bivariate comparison, both age ($p = .004$)[95] and frequency of the Internet use ($p < .001$) show significant effect on the opinion. When controlling for frequency of the Internet use, material status, and education, age is shown as the only significant factor, suggesting that older users are more likely to blame the governments than themselves in case of the breach.[96]

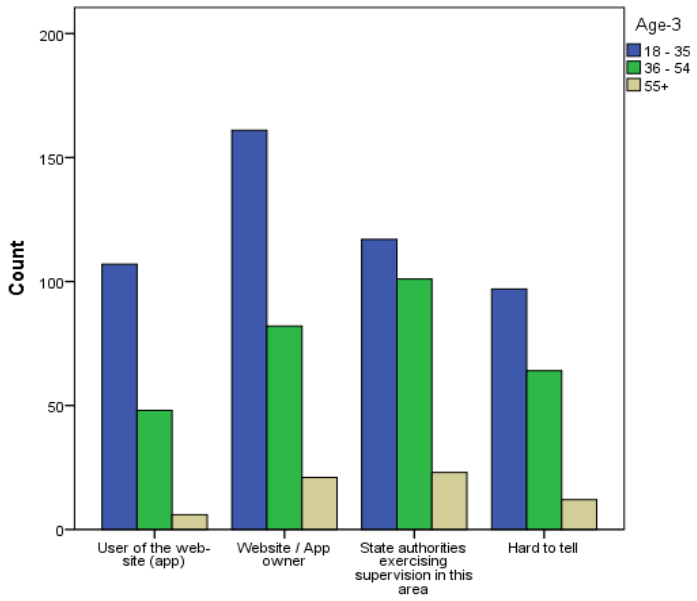

Chart 14. *Who do you think is often to blame for breach of privacy: user, website / app owner, or state authorities exercising supervision in this area?*

H4: The younger generation demonstrates a different privacy risk attitude and behavioral pattern (PARTIALLY HOLDS).

In support of Hypothesis 4, there is evidence that the younger generation demonstrates a different privacy risk attitude and behavioral pattern.

[95] Would be significant at the 95% confidence level
[96] See Table 2.8 in Appendix 2.

It is of no surprise that younger audience uses the Internet more often.[97] They are prone to share more as demonstrated through an attitudinal trend towards social networks as a public space rather than a private space ($p = .002$)[98]. At the same time, however, they demonstrate a higher likelihood of protecting their privacy compared to an older audience, by engaging in practices such as reading the privacy policy of the web-site, checking the security level of the web site, clearing the computer's searching and browsing history, and adjusting social network's settings. This may also signal a better knowledge of various instruments to mitigate risks and protect privacy.

As was demonstrated above, age has a significant effect on putting blame on third parties or oneself. Younger users tend to blame users (that could mean themselves) rather than state authorities or website / app owners in case of privacy breach.

Age shows no significant effect on either an overall feeling of worry about the protection of personal data online, or the increase of that feeling in the last year. I therefore submit that the hypothesis partially holds.

6. CONCLUSIONS

Internet privacy regulation in Russia has been through a great transformation, from general regulatory framework developed mostly for offline environment to specific and detailed norms regulating exclusively privacy practices on the Internet. As the level of users' privacy concern contributes greatly to the privacy regulatory model, this study has tried to get a better understanding of what that level of concern is, and how it is exhibited through users' privacy behavior.

[97] N=839, rho=.259, p < .001
[98] N=689, rho=.118, p=0.002

As the study demonstrates, the level of privacy concern in Russia is rather mixed: users are divided equally on whether they feel worried or not about the confidentiality of their personal data online. They also don't demonstrate a clear trust preference in online or offline environments as far as the protection of their data is concerned. Their level of worry about online privacy in the last year has significantly increased, and that increase could have been triggered by media coverage of many recent privacy leaks. Users' knowledge of specific types of exposure (*e.g.*, passive data collection or targeted advertising) may not be fully complete, and their privacy behavior does not always match their attitude (users demonstrating tendency toward more privacy do not necessarily take appropriate steps to protect their data). In a strict government regulation model, which Russia is, users generally prefer to put more blame on the government and Internet businesses, than on themselves, when they experience privacy breaches. This in turn may make users less motivated to learn about and take proactive actions to protect themselves.

The results of the users' awareness of data collection practices (or a lack thereof) provides some support for advocating for more privacy educational campaigns, rather than a strict government regulation model, that would help users make informed decisions. But even then, web sites should be required by way of a government regulation and / or industry code to disclose to users their data collection practices in a transparent way. In addition, policy makers may want to promote those services that assist users in understanding which of their data is being used, as well as maintaining control over that information.[99]

Interestingly enough and despite a common belief that young people do not care about their privacy, there is evidence that the younger generation is not indifferent to their privacy and their identity. They demonstrate a willingness to share more, but they are more knowledgeable

[99] For example, online service Datacoup helps aggregate, package and sell personal data, allowing users to both better monetize their data and have a peace of mind about how it is used. (https://datacoup.com/#intro). Another example is Handshake - an app and a web site that allows users to negotiate a price for their personal data directly with the companies that want to buy it. (http://www.handshake.uk.com/hs/index.html).

and demonstrate stronger privacy behavioral patterns when it comes to the protection of their data. Therefore, both policy makers and businesses should be targeting their educational campaigns more precisely by putting a greater focus on the older Internet population.[100]

As Internet penetration and the frequency of Internet use will undoubtedly increase, based on the observed dependencies in the study, some of the identified shortages may take care of themselves: users will be more likely to notice targeted advertising, apply protective measures, and pursue certain legal enforcement paths.

In a data - rich economy, privacy can become a tradable commodity. This study shows that a significant amount of users state that they may prefer to avoid the transaction if they perceive the risks to their data as too high. Although this stated choice is subject to limitations and may not always necessarily match these users' actual behavior,[101] at a minimum there is an opportunity for the Internet businesses to adjust their business practices for their own benefit. The users in question tend to have a higher material status and businesses might be interested in exploring the opportunity of letting these users pay to avoid the disclosure of information for certain purposes while still using a service.[102] Alternatively, the businesses may offer users more choice and control over what personal information they share.[103]

Although users did not demonstrate a prevailing trust in either foreign or local Internet as of the day of this study, the situation will likely change by the end of 2014 and beyond. The government is in the process of implementing new legislative initiatives that require all Internet

[100] As an example of such effort, Google launched an educational campaign in the city of Nizhny Novgorod, Russia in 2012 called "Get your grandma and grandpa online". The campaign not just explains the basics of the Internet, but also teaches basic Internet safety skills.
[101] When selecting this option users may state their abstract intentions, rather than actual behavior. See more on this in the section *"Privacy paradox"* above.
[102] Think for example of a paid Gmail version option, under which user's email content is not automatically indexed by Google and user is not shown targeted ads.
[103] For one of such examples, see *Introducing Anonymous Login and an Updated Facebook Login*, Apr. 30, 2014, available at https://newsroom.fb.com/news/2014/04/f8-introducing-anonymous-login-and-an-updated-facebook-login/ (at its last f8 developers conference Facebook announced an option of anonymous logins with better privacy controls).

businesses processing personal data of Russian users to place servers within the territory of Russia and to cooperate with law enforcement authorities as to the provision of users' data.

Additional research initiatives will need to be undertaken in order to better understand the development of privacy concerns in Russia over time. In addition, the effect of societal values, which are currently experiencing a major transformation in Russia, on privacy expectations and online behavior will need to be studied.

APPENDIX 1. INTERNET AUDIENCE

Table 1. Characteristics of Internet users (combined, average, based on two groups)[104]

		n	%
Gender	Male	753	46,5
	Female	867	53,5
Material status	Level 1	81	5
	Level 2	312	19,3
	Level 3	755	46,6
	Level 4	362	22,3
	Level 5	93	5,7
	Level 6	17	1
Education	Primary	35	2,2
	Secondary (general)	422	26
	Secondary (specialist)	591	36,5
	Higher	571	35,2
Profession	Businessman (enterpreneur, farmer)	39	2,4
	Senior executive	8	0,5
	Department head	66	4,1
	Specialist	364	22,5
	Employee	255	15,7
	Worker	401	24,8
	Unemployed pensioner	114	7
	Unemployed and don't plan to look for a job	92	5,7
	Unemployed but looking for job	113	7

[104] The two groups were homogeneous and did not differ significantly on any demographic variable

	Student	140	8,6
	Other	28	1,7
Place of residence	Moscow	162	10
	City with population 1mln+	261	16,1
	City with population 250K-1mln	295	18,2
	City with population 50K-250K	289	17,8
	Towns with population <50K, townships	305	18,8
	Village	308	19
Age		Mean= 35.26 (std. dev. 12.7)	Range: 18-88
Total		**1620**	

APPENDIX 2. REGRESSIONS

Table 2.1

Awareness: *What proportion of websites/smartphone apps do you think collect information about the people who visit/use them?*

Observation: Those who gave "Hard to tell" response (that could signal a lack of knowledge) are also likely to choose not to complain.

Classification Table[a]

			Predicted		
			If your privacy were breached, would you complain, and if yes - to whom? (Up to 3 responses) / Would not complain		
	Observed		0	Would not complain	Percentage Correct
Step 1	If your privacy were breached, would you complain, and if yes - to whom? (Up to 3 responses) / Would not complain	0	591	0	100,0
		Would not complain	248	0	,0
	Overall Percentage				70,4

a. The cut value is ,500

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	hard_to_tell_passive	-,597	,180	10,988	1	**,001**	,550
	Constant	,197	,328	,362	1	,548	1,218

a. Variable(s) entered on step 1: hard_to_tell_passive.

Table 2.2.

Awareness: *What proportion of websites/smartphone apps do you think collect information about the people who visit/use them?*

Observation: Those users who gave “Hard to tell” response tend to be less frequent Internet users.

Classification Table[a]

			Predicted		
			hard_to_tell_passive		Percentage
	Observed		1,00	2,00	Correct
Step 1	hard_to_tell_passive	1,00	0	167	,0
		2,00	0	672	100,0
	Overall Percentage				80,1

a. The cut value is ,500

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	**Internet use**	,484	,157	9,526	1	**,002**	1,622
	Constant	,074	,431	,030	1	,863	1,077

a. Variable(s) entered on step 1: internet_use.

Table 2.3.

Awareness: *At the moment many web sites use targeted advertising, based on the user's activity online, i.e. his search queries, visited sites, email content, etc. Do you or do you not notice advertising that is targeted at you, that takes into an account your search?*

Observation: More frequent Internet users and users with a higher level of education are more likely to notice targeted ads.

Classification Table[a]

			Predicted		
			Targeted advertising		
	Observed		Don't notice	Notice (incl hard to tell)	Percentage Correct
Step 1	Targeted advertising	Don't notice	116	224	34,1
		Notice (incl hard to tell)	101	340	77,1
	Overall Percentage				58,4

a. The cut value is ,500

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	**Education**	,329	,088	13,958	1	**,000**	1,389
	Age	,037	,117	,098	1	,755	1,037
	Internet use	,467	,154	9,252	1	**,002**	1,596
	Gender	,109	,151	,523	1	,470	1,115
	Material status	,076	,074	1,050	1	,306	1,079
	Constant	-2,483	,615	16,279	1	,000	,083

a. Variable(s) entered on step 1: Education, Age, Internet use, Gender, Material status.

Table 2.4

Attitude: *Overall, do you feel worried about confidentiality of your personal data online?*

Observation: Material status has the strongest (negative) effect on the feeling of worry, while a higher level of education contributes to more worry.

Classification Table[a]

			Predicted		
			worry		Percentage
	Observed		not worried	worried	Correct
Step 1	worry	not worried	198	162	55,0
		worried	159	203	56,1
	Overall Percentage				55,5

a. The cut value is ,500

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Age	,010	,121	,007	1	,933	1,010
	Education	,240	,090	7,199	1	**,007**	1,272
	Internet use	,165	,160	1,075	1	,300	1,180
	Material status	-,300	,076	15,608	1	**,000**	,741
	Constant	-,280	,581	,232	1	,630	,756

a. Variable(s) entered on step 1: Age, Education, Internet use, Material status.

Table 2.5.

Attitude*: Social networks: private or public space?*

Observation: Female users, and older users tend to view social networks as private space

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1,357	,152		8,929	,000
	Gender	-,077	,037	-,081	-2,089	**,037***
	Age	-,062	,029	-,082	-2,108	**,035***
	Education	-,011	,012	-,034	-,874	,383
	Material status	,006	,020	,011	,289	,773
	Internet use	,073	,040	,071	1,843	,066

a. Dependent Variable: If you use social networks, this is for you a private space, where you share information with your relatives and friends, or a public space - where you share information with all users of this social network?

* Would be significant at the 95% significance level

Table 2.6.

Behavior: *What of the following actions you would have to take to protect your privacy online?*

Observation: Higher material status contributes most to the likelihood of choosing not to use a web site / smartphone app / service because of the information requested in order to use it

Classification Table[a]

			Predicted		
			Choose not to use a web site / smartphone app / service because of the information requested in order to use it		
	Observed		0	Read privacy policy prior to providing personal information	Percentage Correct
Step 1	Choose not to use a web site / smartphone app / service because of the information requested in order to use it	0	662	0	100,0
		Choose not to use a web site / smartphone app / service because of the information requested in order to use it	176	0	,0
	Overall Percentage				79,0

a. The cut value is ,500

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Internet use	,049	,186	,068	1	,794	1,050
	Material status	,261	,097	7,278	1	**,007**	1,299
	Occupation	-,040	,043	,888	1	,346	,960
	Education	,183	,117	2,448	1	,118	1,201
	Age	-,212	,148	2,043	1	,153	,809
	Constant	-2,312	,847	7,446	1	,006	,099

a. Variable(s) entered on step 1: Material status, Internet use, Occupation, Education, Age.

Table 2.7.

Behavior: *What of the following actions you would have to take to protect your privacy online?*

Observation: Younger, richer and more frequent Internet users are more likely to take certain actions to protect their privacy (*e.g.*, adjust privacy settings on social network, or check the security of the web site).

Classification Table[a]

			Predicted		
			What of the following actions you would have to take to protect your privacy online? (Any number of responses) / Adjust privacy settings on social networking site		
	Observed		0	Read privacy policy prior to providing personal information	Percentage Correct
Step 1	What of the following actions you would have to take to protect your privacy online? (Any number of responses) / Adjust privacy settings on social networking site	0	746	0	100,0
		Read privacy policy prior to providing personal information	92	0	,0
	Overall Percentage				89,0

a. The cut value is ,500

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	**Age**	-,467	,215	4,723	1	**,030***	,627
	Internet use	,999	,391	6,518	1	**,011***	2,715
	Education	,204	,144	1,989	1	,158	1,226
	Material status	,543	,126	18,520	1	**,000**	1,722
	Constant	-6,713	1,330	25,460	1	,000	,001

a. Variable(s) entered on step 1: Age, Internet use, Education, Material status.

* Would be significant at the 95% significance level

Classification Table[a]

			Predicted		
			What of the following actions you would have to take to protect your privacy online? (Any number of responses) / Check the security level of the web-site / app		
	Observed		0	Read privacy policy prior to providing personal information	Percentage Correct
Step 1	What of the following actions you would have to take to protect your privacy online? (Any number of responses) / Check the security level of the web-site / app	0	709	0	100,0
		Read privacy policy prior to providing personal information	129	0	,0
	Overall Percentage				84,6

a. The cut value is ,500

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	**Age**	-,383	,177	4,682	1	**,030***	,682
	Internet use	,568	,264	4,611	1	**,032***	1,764
	Education	,009	,121	,006	1	,941	1,009
	Material status	,291	,108	7,294	1	**,007**	1,338
	Constant	-3,712	,941	15,549	1	,000	,024

a. Variable(s) entered on step 1: Age, Internet use, Education, Material status.

* Would be significant at the 95% significance level

Table 2.8.

Hypothesis 1: *NSA / Snowden scandal last year significantly affected users' attitude (HOLDS)*

Observations:

1. A higher material status contributed to less worry in the last year.
2. People who feel more worried have also likely become more worried in the last year

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2,185	,119		18,331	,000
	Internet use	-,012	,033	-,013	-,382	,703
	Education	,024	,018	,045	1,320	,187
	Age	,004	,025	,006	,173	,862
	Material status	-,071	,015	-,159	-4,667	**,000**
	Overall feeling of worry	,408	,032	,439	12,941	**,000**

a. Dependent Variable: In the last year were you worried more or less about confidentiality of your personal data, or the same?

Table 2.9.

Hypothesis 3: *In a paternalistic (highly regulated) model, users tend to put more blame on the government or Internet businesses, than on themselves, in case of privacy breaches*

Observation: Older users are more likely to blame the government or web-site / app owner, not themselves, in case of privacy breach.

Classification Table[a]

			Predicted		
			blame_state_website_owner		Percentage
	Observed		,00	1,00	Correct
Step 1	blame_state_website_owner	,00	0	161	,0
		1,00	0	504	100,0
	Overall Percentage				75,8

a. The cut value is ,500

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Internet use	-,238	,215	1,231	1	,267	,788
	Material status	-,016	,103	,023	1	,879	,984
	Occupation	-,017	,044	,154	1	,695	,983
	Education	-,060	,122	,246	1	,620	,941
	Age	,400	,162	6,078	1	**,014***	1,492
	Constant	1,566	,905	2,994	1	,084	4,785

* Would be significant at the 95% significance level

APPENDIX 3. SURVEY QUESTIONS

Group 1.

1. Which of the following data cannot be used without your permission? (any number of responses)

a) Name
b) Home address
c) Date of birth
d) Your current location
e) IP address of your computer
f) Your pictue
g) Your car license plate
h) Your tax identification number
i) Your passport number
j) You telephone number
k) Your mobile telephone number
l) Your work telephone number
m) Your placed phone calls
n) Your email address
o) Content of your emails
p) Name of your employer
q) Web sites you visited
r) Other
s) All of the above cannot be used without my permission
t) All of the above can be used without my permission
u) Hard to tell
v) No response

2. What proportion of websites/smartphone apps do you think collect information about the people who visit/use them? (One response)

a) All or almost all
b) Most
c) About a half
d) Minority
e) None, or only a few
f) Hard to tell
g) No response

3. If your privacy were breached, would you complain, and if yes - to whom? (No more than 3 responses)

a) Would not complain

b) Organisation that is in possession of my data
c) Court
d) Roscomnadzor (Russian Telecom Watchdog)
e) Rospotrebnadzor (Russian Consumer Watchdog)
f) Ombudsman
g) Police / Public Prosecutor
h) Local or state MP
i) Hard to tell
j) No response

4. What of the following actions you would have to take to protect your privacy online? (Any number of responses)

a) Read privacy policy prior to providing personal information
b) Ask questions of organizations as to why particular information is needed
c) Check the security of a web site
d) Clear searching and browsing history
e) Choose not to use a web site / smartphone app / service because of the information requested in order to use it
f) Adjust privacy settings on social networking sites
g) Provide false name
h) Provide false details
i) Other
j) Nothing
k) Hard to tell
l) No response

5. Which of the following, you think, may cause the biggest harm to people like you? (No more than 3 responses)

a) The use of personal information for sending out unsolicited advertising to email / mobile phones
b) Credit card fraud
c) Fraud with electronic payment systems, sms - payments
d) Publication of personal information without permission
e) Hacking of social networks and distribution of personal data (phone number, address, etc)
f) Transfer of personal data abroad for processing
g) Secret access to my data by law enforcement
h) Other
i) Nothing from the above
j) Hard to tell
k) No response

6. Who do you think is often to blame for breach of privacy: user, website / app owner, or state authorities exercising supervision in this area? (One response)

a) User of the website / app
b) Website / App owner
c) State authorities exercising supervision in this area
d) Hard to tell
e) No response

7. Which resources (web-sites, applications) do a better job at protecting personal data of their users: Russian or foreign? (One response)

a) Certainly Russian
b) More likely Russian
c) More likely foreign
d) Certainly foreign
e) Equally Russian and foreign
f) Hard to tell
g) No response

8. If you use social networks, this is for you a private space, where you share information with your relatives and friends, or a public space - where you share information with all users of this social network (One response)

a) Private space
b) Public space
c) Don't use social networks
d) Hard to tell

Group 2.

1. At the moment many web sites use targeted advertising, based on the user's activity online, i.e. his search queries, visited sites, email content, etc. Do you or do you not notice advertising that is targeted at you, that takes into an account your search queries, and online activity? If you do notice -- do you or do you need feel any discomfort in this respect? (One response)

a) Don't notice advertising targeted at me
b) Certainly feel discomfort
c) Rather feel discomfort
d) Rather don't feel discomfort
e) Certainly don't feel discomfort
f) Hard to tell
g) No response

2. Which private information about you is not allowed to be used to target advertising at you? (Any number of responses)

a) My search queries
b) The sites that I visited
c) Information received as a result of the indexing of my emails content
d) My current location
e) Information from social networks
f) It is ok to use any information
g) Hard to tell
h) No response

3. In which of the case you think your personal data is better protected? (One response)

a) When I submit them online
b) When I submit them offline in paper form
c) Personal data is protected equally well online and offline
d) Personal data is protected equally bad both online and offline
e) Hard to tell
f) No response

4. Overall, do you feel worried about confidentiality of your personal data online? (One response)

a) Certainly feel that way
b) Rather feel that way
c) Rather don't feel that way
d) Certainly don't feel that way
e) Hard to tell
f) No response

5. In the last year were you worried more or less about confidentiality of your personal data, or the same? (One response)

a) Certainly more
b) Rather more
c) Nothing changed
d) Rather less
e) Certainly less
f) Hard to tell
g) No response

6. Which of the following resources you use regularly at least once per week? (Any number of responses)

a) Vkontakte
b) Mozilla browser
c) Opera browser
d) Google Chrome browser
e) Gmail
f) Twitter
g) Odnoklassniki
h) Facebook
i) Yandex search
j) Don't use any of these resources
k) Hard to tell
l) No response

7. Which of the following resources do you think do a better job at protecting confidentiality of personal information? (Any number of responses)

a) Vkontakte
b) Mozilla browser
c) Opera browser
d) Google Chrome browser
e) Gmail
f) Twitter
g) Odnoklassniki
h) Facebook
i) Yandex search
j) Don't use any of these resources
k) Hard to tell
l) No response

8. Where did you use the Internet in the last 6 months? (Any number of responses)

a) At home
b) At work
c) At the place of my study
d) At my friends' place
e) At designated places (Internet café, game club, post office, etc)
f) In public places from my personal device (café, restaurant, train station, airport, etc)
g) At any place using mobile network
h) Other
i) Hard to tell

j) Don't use the Internet
k) No response

Demographic questions for both groups

1. Have you ever used the Internet? If yes, when was the last time you used the Internet? (One response)

a) Never used
b) Last 24 hours
c) In the last week
d) In the last month
e) In the last 3 months
f) In the last 6 months
g) In the last year
h) More than a year ago
i) Hard to tell
j) Don't know what the Internet is
k) No response

2. What is your gender?

a) Male
b) Female

3. What is your age?

_____

4. What is the level of your education? (One response)

a) Primary education
b) Secondary education (general)
c) Secondary education (specialist)
d) Higher education

5. What is your employment status? (One response)

a) Employed
b) Unemployed

6. What is your place of residence? (One response)

a) Moscow
b) City with 1+ mln population
c) City with 250K-1mln population
d) Town with 50K-250K population
e) Town with < 50K population
f) Village

BIBLIOGRAPHY

Books

Acquisti, Alessandro & Grossklags, Jens, *What Can Behavioral Economics Teach Us About Privacy?* in *Digital Privacy: Theory, Technologies, and Practices* (2008).

Anand, Paul, *Foundations of Rational Choice Under Risk (*3rd ed. 2002).

Fatyanov A.A., *Pravovoe obespechenie bezopasnosti informacii v Rossiyskoy Federacii* (2001).

Westin, Alan F., *Privacy and Freedom* (1967).

Westin, Alan F., *The Origins of Modem Claims to Privacy*, in *Philosophical Dimensions of Privacy* (1984).

Journal Articles

Acquisti, Alessandro & Grossklags, Jens, *Privacy attitudes and privacy behavior*, Economics of information security 7 (2004).

Altman, Irwin, *Privacy Regulation: Culturally Universal or Culturally Specific?* Journal of Social Issues, 33: 66–84 (1977).

Bennett, Colin J., *Regulating privacy: Data protection and public policy in Europe and the United States* (1992).

Cate, Fred H. & Litan, Robert, *Constitutional Issues in Information Privacy*, 9 Mich. Telecomm. & Tech. L. Rev. 35, 37 (2002).

Debatin, Bernhard, et al., *Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequence*, Journal of Computer-Mediated Communication 15, 83-108 (2009).

Featherman, Mauricio S. & Pavlou, Paul A., *Predicting E-Services Adoption: A Perceived Risk Facets Perspective*, International Journal of Human-Computer Studies, vol. 59 (2003).

Gross, Hyman, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34, 35 (1967).

Hirsch, Dennis,*The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?* Seattle University Law Review, Vol. 34, No. 2 (2011).

McDonald, Aleecia M. & Cranor, Lorrie F., *An empirical study of how people perceive online behavioral advertising*, Tech. Rep. CyLab Technical Report 09-015 (Nov. 2009).

McDonald, Aleecia M. & Cranor, Lorrie F., *Americans' Attitudes About Internet Behavioral Advertising Practices*, in *Proceedings of the 9th Workshop on Privacy in the Electronic Society* (WPES) (Oct. 4, 2010).

Milberg, Sandra J. et al., *Information privacy: Corporate management and national regulation,* Organ. Sci. (2000).

Milberg, Sandra J., et al., *Values, personal information privacy, and regulatory approaches*, Comm. ACM 38 (12) 65–74 (1995).

Moor, James H., *Towards a theory of privacy in the information age*, ACM SIGCAS Computers and Society vol. 27, 27-32 (1997).

Norberg, Patricia A., Horne, Daniel R., and Horne, David A., *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, Journal of Consumer Affairs, 41: 100–126, 101 (2007).

Parker, Richard B., *A Definition of Privacy,* 27 RUTGERS L. Rev. 275, 277 (1974).

Posner, Richard A., *An Economic Theory of Privacy*, AEI Journal on Government and Society, 19-26 (May/June 1978).

Solove, Daniel J., *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002).

Tversky, Amos & Kahneman, Daniel, *Advances in prospect theory: Cumulative representation of uncertainty.* Journal of Risk and Uncertainty, 5 (1992).

Tversky, Amos & Kahneman, Daniel, *Judgment under uncertainty: Heuristics and biases*, Science 185.4157 (1974).

Online publications

Alekseevskih, Anastasia, *Regulyator potreboval ot bankov lusche hranit dannye klientov*, Apr. 8, 2014, *available at* *http://izvestia.ru/news/568804* (last visited May 30, 2014).

Angwin, Julia, *Has Privacy Become a Luxury Good?* N.Y. Times, Mar. 3, 2014, *available at* http://www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html?hp&rref=opinion&_r=1 (last visited May 30, 2014).

Desilver, Drew, *Young Americans and privacy: 'It's complicated', available at* http://www.pewresearch.org/fact-tank/2013/06/20/young-americans-and-privacy-its-complicated/ (last visited May 30, 2014).

Fond Obschestvennoe Mnenie, *Zaschita Personalnyh Dannyh*, May 23, 2013, *available at* http://runet.fom.ru/SMI-i-internet/10922 (last visited May 30, 2014).

Fond Obschestvennoe Mnenie, *Internet v Rossii: dinamika proniknoveniya. Osen' 2013*, Jan. 14, 2014, *available at* http://fom.ru/SMI-i-internet/11288 (last visited May 30, 2014).

Goehner, Duane & Richmond, Yale, *Russian / American Cultural Contrasts, available at* http://www.goehner.com/russinfo.htm (last visited May 30, 2014).

Hoofnagle, Chris J., et al., *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* (April 14, 2010), *available at* http://ssrn.com/abstract=1589864 (last visited May 30, 2014).

Introducing Anonymous Login and an Updated Facebook Login, Apr. 30, 2014, available at https://newsroom.fb.com/news/2014/04/f8-introducing-anonymous-login-and-an-updated-facebook-login/ (last visited May 30, 2014).

Kramer, Andrew, *N.S.A. Leaks Revive Push in Russia to Control Net*, N.Y. Times, July 14, 2013, *available at* http://www.nytimes.com/2013/07/15/business/global/nsa-leaks-stir-plans-in-russia-to-control-net.html?_r=1& (last visited May 30, 2014).

Lessig, Lawrence, *Code is Law: On Liberty in Cyberspace*, *available at*: http://harvardmagazine.com/2000/01/code-is-law-html (last visited May 30, 2014).

Levada-Center, *Tseli i konfidentsialnost rossiyan v Internete*, Nov. 11, 2013, *available at* http://www.levada.ru/11-11-2013/tseli-i-konfidentsialnost-rossiyan-v-internete (last visited May 30, 2014).

Love, Dylan, *Netflix's Recommendation Engine Drives 75% Of Viewership*, Business Insider, Apr. 9, 2012, *available at* http://www.businessinsider.com/netflixs-recommendation-engine-drives-75-of-viewership-2012-4 (last visited May 30, 2014).

Moloney, Maria & Bannister, Frank, *Privacy Control Theory for Online Environments* 5 (August 3, 2009), *available at*: http://ssrn.com/abstract=2227595. Proceedings of the 42nd Hawaii International Conference on System Sciences – 2009 (last visited May 30, 2014).

Moloney, Maria & Poti, Valerio, *A Behavioral Perspective on the Privacy Calculus Model* (2013), *available at* http://ssrn.com/abstract=2310535 (last visited May 30, 2014).

Office of the Australian Information Commissioner, *OAIC Community Attitudes to Privacy survey Research Report* (2013), *available at* http://www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013(last visited May 30, 2014).

Pew Research Center, *Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic*, Jun. 10, 2013, *available at* http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/ (last visited May 30, 2014).

Razumovskaya, Olga, *Russia's Internet Market Predicted to Post Double-Digit Growth*, Wall S. J., Oct. 18, 2013, *available at* http://blogs.wsj.com/emergingeurope/2013/10/18/russias-internet-market-predicted-to-post-double-digit-growth/ (last visited May 30, 2014).

Salcito, Anthony, *Privacy and security rank as college students' #1 concern about online activity, according to new poll*, Sep.25, 2012, *available at* http://blogs.technet.com/b/microsoft_in_education/archive/2012/09/25/privacy-and-security-

rank-as-college-students-1-concern-about-online-activity-according-to-new-poll.aspx (last visited May 30, 2014).

Solove, Daniel, *Do Young People Care About Privacy?* Oct. 10, 2012, *available at* http://www.linkedin.com/today/post/article/20121010201716-2259773-do-young-people-care-about-privacy (last visited May 30, 2014).

Story, Louise, *Company Will Monitor Phone Calls to Tailor Ads*, New York Times, Sept. 24, 2007, *available at*: http://www.nytimes.com/2007/09/24/business/media/24adcol.html (last visited May 30, 2014).

Legislation

The Universal Declaration of Human Rights, 1948.

The European Convention on Human Rights, 1950.

The Charter of Fundamental Rights of the European Union, 2000.

Constitution of the Russian Federation, 1993.

Federal Law On Personal Data #152-FZ, 2006.