EDAM Cyber Policy Paper Series 2

Data Privacy and Surveillance in Turkey:

An Assessment of the Draft Law on the Protection of Personal Data

Asst. Prof. H. Akın Ünver

Faculty Member, International Relations, Kadir Has University

Grace Kim

Research Assisstant, EDAM

19 February 2016

INTRODUCTION

Hyper-connectivity is the norm in today's world, linking people, devices, and networks faster, cheaper, and more conveniently than ever. From portable computers to smartphone watches, technology in the 21st century capitalizes on big data that is rampantly collected and analyzed in our highly digitized world. On one hand, the integration of digital technology into many aspects of our daily lives has made communication, education, and leisure more accessible to billions of people. On the other hand, the ubiquitous use of technology has made our privacy increasingly more vulnerable, subject to government surveillance and cyber hacking.

The delicate balancing act of protecting national security while respecting individual privacy rights has brought the topic of data privacy to the forefront of public debate. The privacy versus security debate has both political and economic dimensions. The political aspects of the debate center around how much leeway national intelligence agencies have in accessing the personal information of citizens and foreign nationals in order to prevent terrorist threats and other potential public incidents from actualizing. Operating covertly in tandem with or without the consent of technology companies that store data on millions of its users on private servers, government-sanctioned electronic surveillance programs continuously check for potential threats by monitoring private computers and phones, often blurring the line between legal surveillance activity and gross violations of individual privacy rights. Many countries guarantee the right to privacy, often enshrined in constitutions and enforced by courts and legislation. The tension between the two considerations spring from disagreement over when privacy violations are justified in order to ensure the greater security of the public and how governments can legally carry out surveillance programs.

The economic aspects of the privacy versus security debate also warrant more widespread discussion. Data privacy is fundamental to the functioning of the modern economy, ensuring that people's personal information is kept private throughout the countless number of international transactions that take place on a daily basis. From shopping online to messaging friends in other countries and from cloud computing to data mining, today's digitally connected world presents new challenges for ensuring privacy protections in order to maintain free and open international markets. The recent annulment of the Safe Harbor agreement, which oversaw data privacy protections for EU-US commercial transactions since 2000, spurred major regulatory changes that were later included in the Privacy Shield agreement between European and American data protection agencies in February 2016.

The age-old debate of privacy versus security took on a new dimension after former NSA contractor Edward Snowden leaked classified documents to the world on June 2013. Since then, governments have been struggling to mitigate public backlash against sanctioned domestic surveillance programs. As the terrorist attacks in cities like Paris and San Bernardino showed, the privacy versus security debate has only grown in importance, placing the onus on governments and citizens alike to maintain the delicate balance between protecting individual freedoms and protecting public safety. Because the Internet often plays the role of an alternative public sphere in which to post grievances, mobilize, and communicate, countries that lack traditional public channels of dissent and political opposition have come to see the expansion of the Internet and digital technology as a threat.

The debate on data access, Internet – social media usage, and privacy became a global mainstream in 2011, as Occupy Wall Street (and its global variants) and the Arab Spring protests rocked the world's major capitals. Rapid access to and dissemination of information through social media outlets such as Twitter, Facebook, Youtube and Instagram both facilitated organizational aspects of these movements, as well as internationalizing their message. The widespread demonstrations and dissident movements of 2011 came to Turkey in 2013, in the form of June protests that began in Istanbul's Gezi Park and spread across other cities through social media, as conventional media was squeezed between the demands of the government and the protesters. It was mainly then that social media, Internet and data policy became mainstream debates in Turkey and acted as new frontiers of communication in state-society relations.

According to World Bank data, Turkey's percentage of Internet users is about 51%.[1] This means that about half of the roughly 80 million people in the country have connected to the Internet through a device such as a computer or mobile phone. The Internet and social media usage increased rapidly in the last decade as well, as part of general economic boom and the increase in purchasing power. While there were only 8,130,188 Internet users in 2003, this figure was 35,358,888 in 2014.[2] Similarly, while the percentage of population penetrated by the Internet was %12.33 in 2003, this figure was %46.64 in 2014.[3] However, it must be underlined that the rapid expansion of the access to the Internet in Turkey is not unique, and

[1] World Bank, 'Internet users (per 100 people)' Accessed 31 January 2016, http://data.worldbank.org/indicator/IT.NET.USER.P2
[2] Internet Live Stats. 'Turkey Internet Users'. Accessed 2 February 2016 http://www.internetlivestats.com/internet-users/turkey/
[3] Ibid

conforms to the global increase in access, as Turkey's share of world Internet users remained at an average of %1.24 through the 2003-2014 period.[4] To that end, Turkey even slipped back slightly in global rank of Internet access; from 15th in 2003, down to 17th in 2014. This is an important and sobering perspective: while much of the problems experienced in Turkey in terms of online freedom of expression or social media restrictions are seen as unique and culture-specific issues, they are nonetheless global issues that are experienced by other countries in their virtual state-society relations, at various levels. Therefore, it is vital to evaluate how Turkey interacts with such concepts as data freedom, personal data or online freedom of expression, within global context.

BACKGROUND

Technological innovations have surpassed what the Internet's original creators could have imagined. Not only has digital and Internet technology drastically transformed our daily lives but it has also revolutionized politics, public opinion, and civic participation. While the Internet itself and the technology companies that discover new ways of utilizing the Internet have sped up globalization and brought disparate world communities closer together, the continued digitization of the world has spurred calls to revisit old legislation and make them applicable to new challenges. For example, the NSA revelations detailing the great extent of government surveillance programs all around the world sparked old debates about how far the government can invade the privacy of its citizens in the name of national security. The encryption debate has also proved to be a major sticking point between federal agencies and tech giants, calling into question whether private companies have a greater duty to the customers that use their services or to the governments that regulate their business.

The privacy versus security debate is comprised of a wide range of stakeholders, including individuals citizens, non-governmental organizations, civil society, academia, businesses, national governments, and intergovernmental institutions. In recent years, Internet Service Providers (ISP) in particular have been at the center of public debate. Unlike individual technology firms, ISPs not only have access to an individual's online activity for a single device or website but also have direct access to the amalgamation of all aggregate online activity across all devices, websites, and applications passing through one Internet connection.

[4] Ibid

These companies have started to realize the profitability of targeted advertising and the possibility of outpacing that of social media companies. In other words, the plethora of digital information collected on the Internet will only continue to grow, placing the onus on governments to put the appropriate privacy safeguards in place.

As Turkey debates the proposed Draft Law on the Protection of Personal Data in Parliament over the next few months, a brief assessment of the privacy legislation in Europe, the United States, China, Russia, and Iran may be useful to frame the liberal as well as authoritarian shades of policy options for the balancing of privacy and national security concerns.

Table 1 - Personal Data Protection: Key Terms[5]

Data	Data means information which – (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
Personal Data	Personal data means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Sensitive Personal Data	Sensitive personal data means personal data consisting of information as to - (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union, (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

[5] Information Commissioner's Office, United Kingdom. 'Key definitions of the Data Protection Act'. Accessed 2 February 2016
https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

Processing	Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including – (a) organization, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data.
Data subject	Data subject means an individual who is the subject of personal data.
Data controller	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Processor	Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Third party	Third party, in relation to personal data, means any person other than – (a) the data subject, (b) the data controller, or (c) any data processor or other person authorized to process data for the data controller or processor.

MAJOR CASE STUDIES

Europe

While many other countries struggle to keep up with the rapid pace of technological change, data European legislation has been explicitly providing data privacy and protection rights for over a decade. The European Charter of Fundamental Rights, proclaimed in 2000 and legally binding to all EU member states, specifically protects rights to privacy, data protection, and effective judicial remedy in the case of wrongdoing. After the Lisbon Treaty went into effect in 2009, data protection became a fundamental right, further cementing European privacy laws against government proclivity for loosening privacy protection mechanisms in favor of more invasive security measures.

Personal data is defined in the European Convention on Human Rights (ECHR) as information that pertains to an "identified or identifiable natural person," the latter being "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[6] Article 8 of the ECHR, which is enforced by European Court of Human Rights (ECtHR), prohibits the processing of personal data except when the data subject gives consent or the data being processed is necessary to pre-approved activities with appropriate safeguards already in place.

In Europe, the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe (CoE) are two other major institutions involved in implementing legal measures to protect personal privacy and data in Europe. The OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (1980) also guarantee privacy rights to individuals, although it is more concerned with the collection, processing, and dissemination of data for international data transfers rather than protection against surveillance. Then in 1981, the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data took privacy rights even further by being the first attempt at applying European privacy rights to new technology. As the Convention's summary states, "This Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data … In addition to providing guarantees in relation to the collection and processing of personal data, it outlaws the processing of 'sensitive' data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards."[7]

Despite these guarantees on privacy, however, the Convention on Personal Data included a caveat that allows the government to invade the privacy of its citizens in the name of national security. According to the Convention, "Restriction on the rights laid down in the Convention are only possible when overriding interests (e.g. State security, defence, etc.) are at stake." Although already applicable to a wide range of technology, neither the OECD Guidelines nor the CoE Convention on Personal Data sufficiently regulates the contemporary challenges facing the delicate balance between privacy and security. However, the EU Data Protection

[6] European Union, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046
[7] Council of Europe, "Details of Treaty No.108" http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

Directive implemented in 1995 and the EU Data Protection Reform proposed in 2012 served as the cornerstones of European digital privacy protection legislation for many years.

On December 15, 2015, the EU Commission, European Parliament, and European Council agreed upon the General Data Protection Reform, which unified fragmented legislation across different countries and sectors into a single legal framework that would form the basis of European data protection regulations if formally adopted.[8] The General Data Protection Regulation and Data Protection Directive are the two main instruments of the Reform. The Data Protection Reform gives Europeans better control over their own personal data and also gives the police and criminal justice system the tools to efficiently access data for ongoing criminal cases while also requiring law enforcement authorities to protect the data of victims, witnesses, and suspects in cases.

The reform package is intended to be a "one-stop shop" and, once formally adopted, will become applicable two years after adoption.[9] Furthermore, companies are now required to notify individuals when their data has been hacked and must grant a "right to be forgotten" for European citizens when specified conditions are met.[10] The General Data Protection Reform also addresses data privacy in relation to small and medium enterprises (SMEs). Because the Reform applies to all 28 EU member countries, the streamlined and easy-to-access data privacy laws are aimed at facilitating cross-border trade and economic development. EU Commissioner for Justice, Consumers and Gender Equality Vera Jourova said, "Citizens and businesses will profit from clear rules that are fit for the digital age, that give strong protection and at the same time create opportunities and encourage innovation in a European Digital Single Market. And harmonised data protection rules for police and criminal justice authorities will ease law enforcement cooperation between Member States based on mutual trust, contributing to the European Agenda for Security."[11]

Although Europe is usually characterized as more privacy-oriented than security-oriented in its policies, the terrorist threat from jihadists returning from the Middle East have led Western liberal democracies to revisit privacy legislation to allow for greater surveillance measures.

---

[8] European Commission, "Agreement on Commission's EU data protection reform will boost Single Digital Market," 15 December 2015, http://europa.eu/rapid/press-release_IP-15-6321_en.htm
[9] European Commission, "Reform of EU data protection rules," Last updated 9 February 2016, http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[10] European Commission, "Questions and Answers: Data protection reform," 21 December 2015, http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm
[11] European Commission, "Agreement on Commission's EU data protection reform will boost Single Digital Market," 15 December 2015, http://europa.eu/rapid/press-release_IP-15-6321_en.htm

According to a *Wall Street Journal* analysis on government requests for user information from technology companies, "Governments and law-enforcement agencies in the European Union made nearly 63,000 requests for information about users to Microsoft, Google Inc., Apple Inc., Facebook and Twitter Inc. in the first half of 2015, up 24% from a year earlier."[12] Despite common perceptions of the EU as a greater advocate for privacy than other Western liberal democracies like the United States, comparisons like these highlight the increasing security measures countries are willing to take under the banner of national security.

United States

The fight against terrorism has renewed debates worldwide, not just in Europe but also in America, on how far governments are allowed to invade the privacy of their citizens in order to ensure their safety. As the inventor and principal maintainer of the World Wide Web, the U.S. wields much influence over the Internet's governance and its regulation, or lack thereof. In a similar vein, the U.S. government also usually prioritizes privacy over security; however, after the terrorist attacks against the Twin Towers on September 11, 2001, it has taken a more security-focused approach in its domestic and foreign policy.

After former NSA contractor Edward Snowden leaked classified documents detailing the U.S. government's extensive domestic surveillance program, Washington suffered relentless criticism from supporters and opponents both domestically and internationally, calling into question the not only the legality but the motives behind anti-terrorism legislation sanctioning greater surveillance powers. Protection against unreasonable search and seizure enshrined in the 4th Amendment of the U.S. Constitution serves as the foundation for all subsequent privacy legislation aimed at shielding citizens from unlawful surveillance practices. According to the U.S. Department of Justice, the Privacy Act of 1974 "[established] a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies."[13] To better protect American citizens, the Electronic Communications Privacy Act of 1986

[12] Sam Schechner, "Tech Companies bring Battle over Data to Davos", *Wall Street Journal* http://www.wsj.com/articles/u-s-tech-companies-bring-encryption-battle-to-davos-1453320950?mod=djem10point&cb=logged0.5909027620218694
[13] U.S. Department of Justice, "Privacy Act of 1974" Accessed 24 January 2016, http://www.justice.gov/opcl/privacy-act-1974

limited law enforcement's access to private communications and penalized disclosures of illegally obtained information.

Perhaps the most controversial and most high-profile piece of legislation granting greater government surveillance authority was the Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, better known as the Patriot Act. The Patriot Act greatly expanded the U.S. government's surveillance powers, giving law enforcement agencies greater leeway and scope in conducting electronic surveillance and roving wiretaps.[14]

After the NSA revelations fomented worldwide outcry against government-sanctioned mass surveillance programs, the already tense relationship between the U.S. government and technology companies soured. In an attempt to start fostering better relations, high-level government officials such as President Obama and Secretary of Defense Ashton Carter have gone to Silicon Valley to meet with tech executives to discuss the White House's digital agenda and potential policy areas of better cooperation. Furthermore, the US Congress passed the Freedom Act in June 2015, which placed more restrictions on government surveillance programs and ended some of the most controversial aspects of the US Patriot Act. Passed one day after the expiration of the Patriot Act, the Freedom Act put an end to the bulk collection of millions of Americans' phone records but still failed to satisfy many privacy advocates who argue that many of the surveillance provisions in the Patriot Act were still in place.[15] After the Freedom Act allowed private companies to take back data storage powers and created a public-interest advocate for secret FISA Court deliberations, some in Congress argued that the US government was giving up too many of its security powers, heightening the possibility of another terrorist attack.[16]

China

Like many authoritarian regimes, China exercises tight control over its domestic Internet and leans strongly in favor of protecting national security - no matter how loosely the term is applied - over protecting the privacy rights of its citizens. While the more than 1 billion

[14] U.S. Department of Justice, "The USA PATRIOT Act: Preserving Life and Liberty" Accessed 28 January, 2016, http://www.justice.gov/archive/ll/highlights.htm
[15] Sabrina Siddiqui, "Congress passes NSA surveillance reform in vindication for Snowden," 3 June 2015, The Guardian, http://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden
[16] Alan Yuhas, "NSA reform: USA Freedom Act passes first surveillance reform in decade – as it happened," The New York Times, 2 June 2015, http://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden

Chinese citizens have long been accustomed to Beijing's unyielding authority over what information, goods, and services are allowed to go in and out of the country, the widespread availability and utility of digitally technology has put increasing pressure on the government to placate the public's desire to connect with the rest of the world.

China operates its Internet infrastructure according to the principle of "cyber-sovereignty," a term coined by President Xi Jinping, to justify internal and external measures. The term *cyber-sovereignty* encapsulates the extension of strict political and economic controls into the digital world, allowing Beijing to "develop, regulate, and manage its domestic Internet" and "to defend its Internet from foreign intrusion and attack."[17] In other words, the Chinese government's firm grip on politics, economics, and society extends to the digital world as well.

In addition to strictly monitoring and regulating citizens' Internet activity, China also exercises firm control over its technological imports and exports, often banning foreign-made products and services under the guise of national security in order to foster the development of its own domestic producers and markets. Beijing cites the radical Islamist threat from the ethnic Uyghurs living in the far western region of Xinjiang as a major impetus for passing security laws increasing state surveillance powers.

Russia

Although the Russian Federation claims to espouse democratic ideals and institutions, the country has implemented increasingly authoritarian measures under the leadership of President Vladimir Putin. The Federal Security Service (FSB), the modern-day successor of the Soviet Committee of State Security (KGB), keeps close tabs on domestic Internet traffic and communication through the System of Operative-Investigative Measures (SORM) program. Starting in the 1980s, the SORM program has been legally intercepting all electronic communication in Russia by coercing network operators and Internet Service Providers (ISPs) into giving the government access to their data and by connecting local FSB bureaus to ISP and telecommunications traffic through thousands of miles of underground cables.

[17] Scott Livingston, "Beijing Touts 'Cyber-Sovereignty' in Internet Governance" Chinafile, 2/19/15, https://www.chinafile.com/reporting-opinion/viewpoint/beijing-touts-cyber-sovereignty-internet-governance

Roskomnadzor is the Russian federal service in charge of supervising the country's telecommunications, information technologies, and mass communication. While Russia claims to uphold democratic ideals in its legislative and judicial policies, the authoritarianism of the Putin regime extends into cyberspace. Over the last few years, Russia has called for national Internets at international forums and espoused the idea that American companies storing data on Russian citizens must build data storage centers on Russian soil.[18]

Pavel Durov is the founder of Vkontakte, Russia's most popular social-networking site. Durov has been at the helm of online opposition to the current government, refusing to give in to information requests on users as well as requests to take down critical pages. "Durov said last year [2014] that he sold his 12 percent stake in Vkontakte amid pressure from Russian authorities, including requests to shut down a page on the networking site dedicated to opposition leader Aleksei Navalny and turn over data about users tied to the 2014 Euromaidan protests that led to the ouster of Ukrainian President Viktor Yanukovych, a Kremlin ally."[19] As evident in the Durov case, Russia continues to exert pressure on social-networking companies and ISPs alike, pressuring them to comply with the government's invasive surveillance policies.

Iran

In Iran, surveillance operates in tandem with censorship as the conservative Iranian government employs both as a way to keep their citizenry under control, control information that could threaten the regime, and protect national security. Popular international social-networking websites, such as Facebook, Twitter, Instagram, and YouTube, are banned but the Iranian government continues to monitor those sites for suspicious activity. A striking example of the paradoxes that govern the country's surveillance programs are epitomized with the existence of Ayatollah Ali Khamenei's multiple social media accounts, the very account banned for the rest of the population.

[18] Julien Nocetti, "Russia's 'Dictatorship-of-the-Law' Approach to Internet Policy" Internet Policy Review Volume 4 Issue 4, 10 November 2015, http://policyreview.info/articles/analysis/russias-dictatorship-law-approach-internet-policy

[19] Golnaz Esfandiari, "Iran's Cyberpolice Call on Internet Giants to Prevent 'Crime' Amid Telegram Concerns" Radio Free Europe Radio Liberty, 5 September 2015, http://www.rferl.org/content/iran-cyberpolice-internet-giants-privacy-concerns/27228394.html

Iran has had a robust surveillance system in place to monitor its citizens ever since the Green Movement protests in 2009. Although Iran's surveillance policies predate the Green Movement, the mass political protests disputing the electoral victory of President Mahmoud Ahmadinejad in 2009 prompted stricter government initiatives to back existing Internet filtering tools with legislation allowing for greater electronic monitoring and information manipulation.[20] Many young people living in Iran's cities joined the Green Movement, leading the government to identify "particular dissidents by tracing their social media use, making inferences based on what they wrote and who they were reading."[21]

Formed in 2012 by direct order of Supreme Leader Ali Khamenei, the Supreme Council on Cyberspace is the highest body that oversees Internet policy in Iran.[22] The body that controls access to online content is the Working Group to Determine Instances of Criminal Content on the Internet. Formed in 2009, the Working Group's members have the approval of Khamenei and are responsible for finding those who post content "supposedly contrary to 'public chastity and morality,' 'sacred Islamic principles,' 'security and public peace,' and 'government officials and public institutions."[23]

Perhaps the most well-known of Iran's surveillance programs is Project "Ankaboot" or Project Spider. Project Spider was first publicly acknowledged by officials on January 31, 2015, but is thought to have been launched in the fall of 2014. The purpose of the program is to "root out Facebook pages and activities that spread 'corruption' and western-inspired lifestyles."[24] The Center for Investigation of Organised Cyber Crimes, which is a subsidiary of the Iran Revolutionary Guards Corps' Cyber Defense Command, runs Spider's operations, acting as a the country's cyber surveillance force. By the end of January 2015, they had shut down 130 Facebook pages, arrested 12 individuals, and detained 24 individuals.[25] While Iran continues to see U.S. tech companies as a threat to the stability of the regime, some American

[20] Irene Poetranto, "Since the Green Movement: Internet Controls in Iran, 2009-2012" Open Net Initiative, 15 February 2013, https://opennet.net/blog/2013/02/after-green-movement-internet-controls-iran-2009-2012
[21] Martin C. Libicki, "Iran: A Rising Cyberpower?" The RAND Blog, 16 December 2015, http://www.rand.org/blog/2015/12/iran-a-rising-cyber-power.html
[22] International Campaign for Human Rights in Iran, "Internet in Chains: The Front Line of State Repression in Iran," November 2014, https://www.iranhumanrights.org/wp-content/uploads/Internet_report-En.pdf
[23] International Campaign for Human Rights in Iran, "Internet in Chains: The Front Line of State Repression in Iran," November 2014, https://www.iranhumanrights.org/wp-content/uploads/Internet_report-En.pdf
[24] Arta Shams, "The State of Surveillance in Iran's Cyberspace" Azad Tribune, 14 May 2015, https://www.article19.org/azad-resources.php/resource/37964/en/the-state-of-surveillance-in-iran%E2%80%99s-cyberspace
[25] Arta Shams, "The State of Surveillance in Iran's Cyberspace" Azad Tribune, 14 May 2015, https://www.article19.org/azad-resources.php/resource/37964/en/the-state-of-surveillance-in-iran%E2%80%99s-cyberspace

companies may be the very ones supplying the regime with the monitoring and blocking technology. The U.S. government has long banned federal contracts to sell this type of technology to Iran, but they "[have] had difficulty in identifying such firms."[26]

Iran's cyber law enforcement groups monitor the Internet for any signs of political opposition and violations of Sharia law. Although many details surrounding the country's surveillance programs cannot be confirmed, Iranian officials like the Chief of Iran's Cyber Police (FATA) have publicly stated that they have been keeping a close eye on users of messaging apps like Viber and Whatsapp.[27] Moreover, Tehran has apparently even managed to pressure highly encrypted messaging apps like Telegram to give into certain national criteria in order to continue operations in the country.[28]

Tehran has taken increasingly drastic steps to tighten its grip on controlling access to and content available on the Internet. With the creation of the National Information Network (NIN), Iran joins other countries in taking definitive steps toward the balkanization of the Internet. Although the NIN was set to be implemented in early 2016, the program has experienced a series of delays, making the date of its completion unclear. Once fully implemented, however, the severe restrictions currently in place will become even stricter. According to a report from the International Campaign for Human Rights in Iran, "all Internet access in Iran will take place through channels accessible to the state, state agencies will have access to all communications inside Iran on the National Internet, the authorities will be able to cut off access to the global Internet at will, and they will also be able to deny or limit access by Internet users abroad to content in Iran's domestic Network."[29] Without the appropriate legislative measures to protect individual privacy rights, the completion of the National Information Network means that all Iranian citizens will be sharing all of their online activity with the country's security, intelligence, and judicial agencies.

As information and communications technology permeates Iranian society like it has the rest of the world, Iranian hardliners will continue to create government mechanisms to monitor its

---

[26] Mario Trujillo, "Firms That Sell Spy Tech to Iran Remain Elusive" The Hill, 13 January 2016, http://thehill.com/policy/technology/265760-firms-that-provide-spy-tech-to-iran-remain-elusive

[27] Arta Shams, "The State of Surveillance in Iran's Cyberspace" Azad Tribune, 14 May 2015, https://www.article19.org/azad-resources.php/resource/37964/en/the-state-of-surveillance-in-iran%E2%80%99s-cyberspace

[28] Golnaz Esfandiari, "Iran's Cyberpolice Call on Internet Giants to Prevent 'Crime' Amid Telegram Concerns" Radio Free Europe Radio Liberty, 5 September 2015, http://www.rferl.org/content/iran-cyberpolice-internet-giants-privacy-concerns/27228394.html

[29] International Campaign for Human Rights in Iran, "Internet in Chains: The Front Line of State Repression in Iran," November 2014, https://www.iranhumanrights.org/wp-content/uploads/Internet_report-En.pdf

citizens online and control digital content. In 2012, Iran passed a law requiring Internet café owners to obtain the first name, last name, father's name, national identification number, post code, and telephone number of each customer.[30] With the signing of the nuclear accord agreements and the opening up of Iran's economy, Iran will inevitably face additional challenges and witness the rising importance of the Internet and digital technology in the lives of its almost 80 million citizens.

EU-US PRIVACY SHIELD AGREEMENT

On October 16, 2015, the European Court of Justice's (ECJ) ruling in the *Maximilian Schrems v. Data Protection Commissioner* case invalidated the US-EU Safe Harbor agreement that had regulated the cross border transfer of personal data between US and EU businesses since 2000. The ECJ ruled that US companies did not provide adequate data privacy protections up to par with European standards and that "legislation permitting public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life."[31] Furthermore, the Court decided that the absence of mechanisms for judicial redress "[compromised] the essence of the fundamental right to effective judicial protection."[32]

On February 2, 2016, almost four months after the annulment of Safe Harbor, the EU Commission and the US agreed on a new data privacy framework for transatlantic data flows called the EU-US Privacy Shield, alleviating the concerns of thousands of businesses stuck in legal limbo after the Safe Harbor agreement was scrapped.[33] There were two main takeaways from the revised Privacy Shield agreement: greater privacy protections and judicial redress mechanisms. Now, US companies and intelligence agencies had greater obligations to protect the personal data of EU citizens, specifically by "stronger monitoring and enforcement by the US Department of Commerce and the Federal Trade Commission, including through increased cooperation with European Data Protection Authorities."[34] With the new

[30] Saeed Kamali Dehghan, "Iran clamps down on Internet use" The Guardian, 5 January 2012, http://www.theguardian.com/world/2012/jan/05/iran-clamps-down-internet-use
[31] Court of Justice of the European Union, "The Court of Justice declares that the Commission's US Safe Harbour Decision is Invalid" (Press Release No. 117/15), 6 October 2015, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf
[32] Ibid.
[33] European Commission, "EU Commission and the United States agree on a new framework for transatlantic data flows: EU-US Privacy Shield," 2 February 2016, http://europa.eu/rapid/press-release_IP-16-216_en.htm
[34] Ibid.

transatlantic data transfer agreement, US public authorities assure that they will no longer "conduct mass or indiscriminate surveillance of Europeans" and that access to the personal data of EU citizens for the purposes of national defense and law enforcement will "be subject to clear conditions, limitations and oversight, preventing generalized access."[35] In other words, US data privacy standards must conform to the stricter data privacy standards of the EU if US businesses want to continue operating in Europe.

The second important takeaway of the Privacy Shield agreement was the creation of judicial redress mechanisms for EU citizens who want to lodge formal complaints against US businesses for handling personal data improperly. For the first time, EU citizens will be able to file formal complaints and inquiries about the privacy of their personal data, which European national data protection authorities will relay to the relevant authorities, and Alternative Dispute resolution will be offered free of charge. Moreover, US companies will have deadlines to reply to complaints, ensuring that individuals do not get tied up in prolonged and expensive legal battles. In order to monitor all the new implementations of Privacy Shield, an annual joint review will be established with members from the European Commission, US Department of Commerce, and invited national intelligence experts from US and European data protection authorities.

Because Turkey aspires to join the European Union, its data privacy legislation must accord with European standards. Turkey should prioritize safeguards against mass surveillance while also taking precautions against using ambiguous justifications like national security to override individual privacy rights. As the Turkish Parliament begins to debate the Draft Law on the Protection of Personal Data starting in February 2016, Turkish citizens and the international community alike must remain vigilant and informed about the ongoing parliamentary debates.

AN ASSESSMENT OF TURKEY'S DRAFT LAW ON THE PROTECTION OF PERSONAL DATA

A Turkey-specific data protection law was first mentioned in 2003, when the EU Accession Partnership Document first mentioned a clause on the matter. The clause was later admitted into Turkey's EU Accession National Programme, but was never drafted into a law. It was

[35] Ibid.

only in December 2014 that the 'Draft Law on the Protection of Personal Data'[36] was finally crafted and was submitted to related EU organs and domestic civil society groups for legal commentary. The resultant amendments were reflected into the revised Draft Law, which was submitted to the Parliament on 18 January 2016.

Before the proposed 'Draft Law on the Protection of Personal Data'[37], there were several existing laws that refer to the collection and use of such data. Primarily, the Turkish Constitution[38], following the amendments of 2010, has rendered the protection of personal data a part of individual rights, introducing restrictions to the state's ability to record and process such data. Such specific Articles of the Constitution are 17 (general acknowledgement of the individual's right of 'living, protection and improvement of his material and spiritual being') and 20 (acknowledgement of the right to 'request the protection of data', including correction and deletion of such data). In Turkish Civil Code[39] on the other hand, Articles 23, 24 and 25 guarantee personal rights, although those that are not specific to online identity or data rights. The Code of Obligations[40] (Law 6098) refers mostly to the financial aspect of data use, as its Article 419 renders employers responsible of their employee's personal data on performance and qualifications. Finally, the Criminal Code[41] Articles 134 (violating secrecy of private data), 135 (illegal recording of data, violation of data collection law, data collection without consent), 136 (transfer and dissemination of personal data) and 138 (data deletion policy and failure in deletion). In addition, the Law on the Right to Access Information[42] allows a degree of access to certain institutional, personal and governmental data, with explicit restrictions on secret data.

There are also sector-specific laws on data protection such as Regulation on Procedures and Principles of Broadcasts via Internet and Regulation on Mass Internet Use Providers, the E-commerce Law, Regulation on Protection and Sharing of General Health Insurance Data, Regulation on Data Privacy and Principles and Procedures Regarding Security of Confidential

[36] Kişisel Verilerin Korunması Kanun Tasarısı. 18 January 2016. http://www2.tbmm.gov.tr/d26/1/1-0541.pdf
[37] Kişisel Verilerin Korunması Kanun Tasarısı. 18 January 2016. http://www2.tbmm.gov.tr/d26/1/1-0541.pdf
[38] Türkiye Cumhuriyeti Anayasası. https://www.tbmm.gov.tr/anayasa.htm
[39] Türk Medeni Kanunu #8049 http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.4721&MevzuatIliski=0&sourceXmlSearch
[40] Türk Borçlar Kanunu. #10757 http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6098.pdf
[41] Türk Ceza Kanunu. #8965 http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf
[42] Bilgi Edinme Hakkı Kanununun Uygulanmasına İlişkin Esas ve Usuller Hakkında Yönetmelik. BDDK. http://www.bddk.org.tr/websitesi/turkce/bize_ulasin/454bilgi_edinme_yon.htm

Data in the Official Statistics, Regulation on Bank Cards and Credit Cards, Regulation on Distance Contracts and the Electronic Communications Law and its secondary legislation.

Assessing the first draft of the Turkish law on data privacy from the perspective of international norms, Nurullah Tekin argues that although Turkey is a member of Council of Europe, United Nations and OECD, it has nonetheless 'failed to incorporate the principles adopted by these organizations in the field of data protection into its domestic law', concluding: 'Turkey still lacks a clear, adequate legal arrangement concerning the processing of personal data'[43]. In the same Article, Tekin points to the fact that Council of Europe views the absence of such law as a serious deficiency in its Turkey Reports, emphasizing that such absence also impacts Turkey's progress in Chapters are 23 (Judiciary and Fundamental Rights), 24 (Justice, Freedom and Security), 10 (Information Society and Media) and 28 (Consumer and Health Protection). In addition, the TUSIAD position report of January 19, 2015[44] emphasizes that the absence of a specific data protection law makes it more difficult to harmonize Turkish and European business and investment practices due to gaps and loopholes in how business, employee and investment data will be processed in times of legal disagreements.

However, in assessing the need for such law, political, rather than purely legal concerns come out as important. First, the multibillion-euro aid package to Turkey to cope with refugees gave an impetus to Turkey – EU relations, including cooperation on data transfers. The need for a law that specifically draws the boundaries on the protection of personal data was thus urgent, as it relates to the transfer of EUROJUST and EUROPOL data between Turkey and the EU to coordinate refugee flow policy. But even before that, Turkey and the EU had launched the Visa Liberalization Dialogue back in December 2013, which proposed a lifting of visa requirements for Turkish citizens traveling into the Schengen area. In the Visa Liberalization Dialogue, two of the seventy-two technical measures were related to data protection conventions. Currently, European Stability Initiative runs an online scorecard on Turkey's

[43] Tekin, N. 'An Assessment of the Turkish Draft Law on Protection of Personal Data in Light of the EU Data Protection Directive'. *Human Rights Review*, Volume:IV, Issue:1, June 2014

[44] 'Kişisel Verilerin Korunması Kanunu Tasarısı Hakkında TÜSİAD Görüşü'. http://www.tusiad.org.tr/__rsc/shared/file/Kisisel-Verilerin-Korunmasi-Kanunu-Tasarisi-Hakkinda-TUSIAD-Gorusu.pdf

performance on the Visa Liberalization Dialogue[45], which shows Turkey's status as '5' (lowest score) in these areas.

ASSESSMENT OF THE DRAFT LAW

The Draft Law on the Protection of Personal Data, defines such data as 'any information that facilitates the identification of persons [including] national identification records, communication, health and financial records, in addition to data related to their personal, religious and political life'. A key justification the draft law lays out as its raison d'étre is to prevent the emergence of a public view that their records are being used in blacklisting. Additionally, the Law proposes that the current legal system does not prevent private and public sector abuse of personal data, including a lack of clarity over who gathers and processes such data. More practically – and perhaps more crucially in terms of the timing of the Draft Law – the justification points the necessity for better coordination between Turkish Police and EUROPOL, which was added before the current scope of the refugee crisis. With the current scale of the refugee problem, the Turkish Police coordination with EUROPOL is more crucial than ever, especially with regard to data sharing on refugee processing. A major element in the justification is a lack of electronic data transfer/cooperation between Turkish and European police departments as Turkey does not comply with the personal data protection requirements of the EU. In addition, the justification points to an increasing number of criminal activities under EUROJUST jurisdiction taking place or transiting through Turkey and that a lack of data privacy framework prevents accurate sharing of criminal data.

In EDAM's assessment, there are two main problems with the Draft Law, as it relates to its main aim: to harmonize Turkey's Data Protection Law with the EU acquis. First, that the independent Data Protection Board, which is introduced by the new Draft Law regressed between the Draft Law's 2014 and 2016 versions. In that regard, the most recent version of the Draft Law significantly jeopardizes the independence of the Data Protection Board by rendering its appointments fully political in motivation, eliminating the technocratic requirement to take part in such a regulatory authority. The second problem is that the wide scope of legal exceptions to the cases on liberties and freedoms introduced earlier in the Draft Law complicates its compatibility with the EU acquis. There is substantial vagueness over

[45] Turkey's Visa Liberalization Roadmap. European Stability Initiative. 17 December 2014. http://www.esiweb.org/index.php?lang=en&id=555

police, gendarmerie or intelligence limits over the processing of personal data, especially with regard to legal barriers and restrictions over the security agencies' liberal interpretation of national security. This becomes an even more pressing issue following the EU-US Privacy Shield agreement, which issues clear cut limits on how US intelligence agencies can process or store EU-origin private data. The same consideration will inevitably be reflected on EU expectations from the Turkish Draft Law.

Table 2 - Turkish Draft Law at a Glance

Definition of Personal Data	Any form of information that may reveal personal identity, communication details, health and financial information, along with religious, private and political views.
Justification of Law	- Use of personal data may be abused by the private and public sector - Handling of such data by unauthorized individuals may lead to leaks, mishandling, infringing upon the Constitution and international treaties Turkey is bound by. - Necessity of establishing a reasonable legal middle ground between unrestricted data flows to facilitate business and preventing abuse of such data. - No law or oversight mechanism exists on the use and handling of personal data, which generates common suspicion over the use of such data. - Necessity to harmonize Turkish data protection laws with that of developed countries. - New law required in order to harmonize police and security coordination and electronic transfer of intelligence between Turkish enforcement agencies and EUROPOL. Similarly, coordination with EUROJUST is impaired due to incompatible legal framework on sharing intelligence, preventing joint enforcement operations. - Growing volume of personal data stored by health

	institutions increasingly problematic as these institutions don't have a legal basis or adequate security framework for the storage of such data. ECHR designates this gap as an infringement on the personal privacy. - Difficulties in sharing personal data of Turkish citizens living abroad, in terms of their conscription, citizenship and financial assets, which complicates their legal standing in Turkey. - Insufficient personal data protection law impairs foreign direct investment and management of foreign capital within Turkey. Such legal gap deters investors to expand investment and business in Turkey, as well as restricting business partnerships of Turkish businessmen abroad.
Existing legal framework	- Turkish Criminal Code #5237 – Article #135: Illegal collection and exposition of personal data Diagnosed Problem: Legal confusion and gap over when such acts constitute legal or illegal practice. - Constitutional Amendment (2010 Referendum) to Article #20: Protection of personal data is considered as a basic human right - European Union Accession Framework: Four Chapters of Accession Negotiations are related to the protection of personal data. A new, specific law on the protection of personal data is required to make progress on these four chapters. - Protection of personal data is pledged as a response to Turkey's 2003 response to EU Accession Partnership Document - 64th Government program has issued an Urgent Action Plan, which pledges reform on protection of personal data within three months. - Turkey is a signatory to OECD's 1980 Guidelines on the

	Protection of Privacy and Trans-border Flows of Personal Data - Turkey is a signatory to Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) in 1981. - Turkey is a signatory to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

The addition of the condition of 'explicit consent' (Article 3, clause b) is a major change in the new draft law, which didn't exist in earlier version of the law. The new law makes a vague emphasis on personal consent and individual's ability to express consent as the basis of personal data processing, outlining a number of exceptions to the rule of requiring express consent. These exceptions (Article #5) are:

a) Existence of a conflicting law
b) Individual's inability to express consent – either through physical difficulty or legal restrictions on the expression of such consent, or in cases where processing personal data is required to protect the physical security of the person in question, or another person.
c) In cases where processing of personal data is required to establish or practice another convention or contract,
d) In cases where the official authorized to process personal data is legally required to do so,
e) In cases where personal data is disclosed or made public by the individual,
f) In cases where processing personal data is required to establish, exercise or protect another right,
g) In cases where processing personal data is required for the legitimate interests of the authorized individual processing the data, as long as it does not infringe upon the fundamental rights and freedoms of the person in question.

To that end, the law brings a large number of conditions and restrictions to the protection of personal data. A major critique of Article #5 would be that it renders the new law

incompatible with international conventions or the EU law, both of which are cited as a major justification for the law in the first place. Furthermore, these exceptions restrain the new law too much and attach it to the existing Turkish legal system in a way that the new law may be deemed insufficient by the related EU agencies in terms of better flow of data.

Article #6 of the law imposes further restrictions on the intended freedoms by listing exceptions on the Processing of Private Personal Information (PPI) and other sensitive data. The Article establishes that data, which contains an individual's 'racial, ethnic, political, philosophical, religious, sectarian – or related to other beliefs, dress and attire, association, membership, syndicate affiliation, health, sexual, criminal and biometric information' cannot be processed 'without sufficient protective measures' or 'express consent of the individual'. However, the Article brings five additional restrictions on processing of such sensitive information in cases where:

a) Another law explicitly requires processing of sensitive data,
b) Political parties, unions, associations, syndicates and other non-profit organizations require processing of such data in accordance with their internal laws, provided that processing of data is related strictly to these associations' field of operation
c) Sensitive data is made public or accessible by the individual in question
d) Processing of such data is required for the establishment, exercise or protection of another right
e) Such processing is required for the planning, administration and financing of health-related activities such as protection of public health, preventive medicine, medical diagnosis, treatment and care – by institutions and persons that are bound by secrecy laws

The law introduces the right to retract, delete and anonymize personal data as well (Article #7), although the terms under which such actions can take place are referred to other existing laws and additional-prospective bylaws. This renders the Article and the proposed law itself insufficient as a standalone legal framework on such matters. A similar problem exists with Article #8, where sharing personal data with third party sources are banned, but then the same exceptions on Article #6 are introduced (except condition 'b'). The nature of exceptions mentioned in Articles 5, 6, 7 and 8 are further problematic as they restrain the new law too much with existing Turkish legal anchors, rendering the new law problematic as a source of legal progress or fulfilling the reasons outlined in the law's justification text.

Articles #10, 11, 12 clarify the gaps in earlier articles by bringing in additional rights and responsibilities on personal data and the authorized party, which processes such data. According to Article #10, the data authority has to provide:

a) The identity of the authorized individual(s) that will process the data of the individual whose personal data has to be processed
b) The reason for the processing of such data
c) To whom and with what purpose personal data may be disclosed to third parties
d) The methodology of data collection and its legal basis
e) To inform the individual whose personal data will be processed on his/her rights, that are outlined in Article #11

Such rights are defined in Article #11 as the individual's right to;

a) be informed whether his/her personal data is processed
b) ask for further information about the details of the processing
c) be informed about whether the processing of personal data is used according to intended purposes and what these purposes are
d) be informed about which third parties will receive processed personal data,
e) ask for correction and editing, if personal data are processed badly or inadequately
f) ask for deletion or retraction of personal data (in accordance with Article #7)
g) inform third parties on the changes outlined in 'e' and 'f'
h) object to the negative result that emerge with the processing of personal data through automated systems
i) request compensation if illegal processing of personal data result in injury

The following Article #12 then imposes a number of responsibilities on the data authority, including prevention of mishandling and bad processing of personal data and taking necessary precautions that such mishandling and bad processing don't take place. In cases of such improper handling, the data authority is required to notify the higher authority, as well as the Personal Data Protection Council.

In cases of mishandling of data, the Law directs the legal complaint first to the data authority, who is obliged to respond within 30 days and may require an additional fee if necessary. The law does not make it clear in regards to who will deem such fee necessary, which is one of the

clauses that will create additional confusion in actual practice. It is then suggested that if data mishandling is the mistake of the data authority, then such fee will be reimbursed. However, it is only when the data authority rejects or becomes unable to resolve the complaint that the individuals can appeal the Personal Data Protection Council, which is authorized to pay legal compensation to the individual in question. The Council is authorized to respond to complaints in the form of making additional documents available within 15 days, enforcing legal practice on the processing of personal data upon the data authority and restrict the transfer of such data to international third parties in required cases.

Another critical part of the Draft Law is the section, which defines the composition of the Data Protection Authority, which will be brought under the jurisdiction of the Prime Minister's Office. The Board is planned as a seven-seat assembly, made up of private or public service veterans with at least ten years of experience and a graduate of a four-year higher education body. The most critical part of the Board is that 4 of its members will be appointed by the Council of Ministers and 3 will be appointed by the President. This is a substantial change since the 2014 version of the same Draft Law, which had a more technical requirement of: two judges or attorneys with at least 10 years of legal experience, one member of the academia with 10 years of higher education experience and four members appointed by the Council of Ministers, provided that they have at least 10 years of experience in public or private sector. This means that the new law changes the technocratic nature of the Council, rendering its technical slots dependent on Presidential preferences. The appointees will serve for a period of four years, after which they may get re-elected, or may be replaced by another appointee that will complete their 4-year tenure. The composition of the Data Protection Authority is one of the main problems of the Draft Law as it stands. First of all, the election mechanism of the board is vague and does not guarantee transparency or merit as it stands. Second, the allocation of four slots to Council of Ministers appointment and three slots to Presidential decision renders the Board incompatible with existing EU law from a political independence standpoint. This is even a step back from the 2014 Draft Law where three slots were dedicated to independent industry or academia specialists.

A final unresolved problem that persists in both 2014 and 2016 versions of the Draft Law is the extent and limits to the use of personal data by police and intelligence agencies. One of the problematic exceptions woven into the Draft Law is the issue of 'preventive, protective and intelligence activities' and cases of 'national security'. The general and unclear wording

of these exceptions endanger the enforcement aspect of the law and risk a very wide interpretation of such terms, potentially leading to more restrictive application of the Draft law. While security issues do bring a legitimate set of exceptions in the EU acquis, Turkish Draft Law still needs to find the right balance in terms of freedom of online expression and privacy, and national security. This is especially critical from the perspective of the most recent EU-US Privacy Shield agreement. One major motivation for the EU to cancel Safe Harbor and renegotiate the deal was to get additional guarantees from the US that the data of EU citizens will not be syphoned off by US intelligence agencies. As a result, the very wide scope of freedom granted to Turkish public authorities and agencies in the Draft Law is likely to generate the same concerns and render it fundamentally incompatible with the EU acquis in its fundamental logic. If cross border data transfers between Turkey and the EU are to be enabled, the Turkish legislation should incorporate guarantees as per under Turkish law for public authorities to access personal data will be subject to clear conditions, limitations and oversight, preventing generalized access and abuse.

Table 3 - Comparison of 3 Major Assessment Reports of the Draft Law

Tekin (2014) Assessment of the 2014 Draft Law	**TUSIAD (2015) Assessment of the 2014 Draft Law**	**EDAM (2016) Assessment of the January 2016 Draft Law**
Definitions of some concepts in the Draft are different, broader or more stringent than those of the EU Directive. As it is, the Draft Law does not harmonize Turkish law with the EU law	Draft Law largely convergent with the European Commission's Data Protection Directive 95/46/EC, but it needs to take European Commission's Proposal 2012/0010 (COD) into consideration.	Article #5 renders the new law incompatible with international conventions or the EU law, both of which are cited as a major justification for the law in the first place.
Processing of personal data will be organized with a specific framework law. This	Draft Law needs to add 'free movement [of people/ goods/ services]' into its aims in	Exceptions restrain the new law too much and attach it to the existing Turkish legal

is a positive intention, but needs to be developed further	order to harmonize better with the EU law.	system in a way that the new law may not fulfil the kind of legal harmonization Turkey hopes to achieve with the EU.
Personal data should be processed only with the explicit consent of the data subject with proper and sound legal exceptions.	Draft Law has to add 'open consent' as a key factor in processing personal data	The law introduces the right to retract, delete and anonymize personal data as well (Article #7), although the terms under which such actions can take place are referred to other existing laws and additional-prospective bylaws. This renders the Article and the proposed law itself insufficient as a standalone legal framework on data processing and transfer.
Positive that it introduces the prohibition of the processing of special categories of data.	Draft Law unclear over what exactly constitutes personal data becoming 'public knowledge'. This endangers legal consent as a key factor in data processing.	The nature of exceptions mentioned in Articles 5, 6, 7 and 8 are further problematic as they restrain the new law too much with existing Turkish legal anchors, rendering the new law problematic as a source of legal progress or fulfilling the reasons outlined in the law's justification text.

Rights such as obtaining information and correction are provided to the data subjects, which improves the Draft Law's transparency	Lack of clarity over who exactly constitutes 'data processor', including which specific state agencies or government authority is legally responsible on this	There are technical problems with the composition of the Council on the Protection of Individuals with Regard to the Processing of Personal Data. With 4 members appointed by the Council of Ministers, and 3 appointed by the Presidency, the Council drift too far away from technical competency and emerges as a political body. This may further impair the Draft Law's ability to harmonize Turkish data protection law with the EU laws.
Data transfer to third countries is restricted. This needs to be developed further to improve security and enable greater business transactions simultaneously.	Draft Law Brings too much responsibility on the data processor, which may increase the chances of increasing unforeseen legal or financial risk	There are still a number of areas where the proposed provisions diverge from the EU legislation and practice. The independence of the data protection authority and the wide scope of exceptions introduced in the law are to be seen as the major points of divergence.
Administrative and criminal sanctions have been provided on the data processor, which	The law makes redundant emphasis on the punishment on violations, that are already	A second major area of incompatibility with the EU acquis relates to the wide

renders him/her responsible.	defined well by the Penal Code	scope of exceptions set out in the draft law (Art 28). Accordingly the law's provisions will not be applied in respect of activities related to national defense, national security, public order and security and even economic security.
An independent Data Protection Board will be established, which will allow a specific board to administer the rules in the Draft Law	It is imperative that the candidates for the Council should be selected among those with experience in protection of personal data, privacy and data security.	It is unlikely that under its current form, the Turkish Law will be seen as being compatible with the EU acquis. So unless it is significantly amended in Parliament, the risk is that Turkey will adopt this law which then will not be seen as having fulfilled the requirement of EU compatibility.
In relation to the implementation of the Law, there are exceptions for areas such as intelligence and judicial activities.	Instead of appointed by the Council of Ministers, the Council of experts must be appointed by the Parliament, with super-majority	If the Draft Law is accepted in the Parliament, EU will not be able to categorize Turkey as a safe country for the purposes of cross border data transfers.

CONCLUSION AND POLICY RECOMMENDATIONS

- Exceptions to the Articles that deal with personal freedoms and privacy should be relaxed in accordance with EU regulations.
- The right to retract, delete and anonymize personal data (Article #7) has to be clearer and better structured legally. The fact that the law introduces another prospective legal text or regulation to determine the scope of this particular Draft Law is problematic from a legal point of view. This Draft Law has to establish the full scope of freedoms and obligations related to the subject matter, without the prospect of another law rendering this Draft Law *a posteriori* ineffectual.
- Concerns about the technical nature of the Council on the Protection of Individuals with Regard to the Processing of Personal Data have to be addressed. As it stands, the Draft Law does not guarantee that the appointees of these positions will be chosen by merit, experience or knowledge – and raises questions over whether these posts will be awarded with political considerations.
- Likewise, the independence of the data protection authority is in jeopardy. Direct nominations for the Board from the judiciary, academia and trade bodies should be considered. A politically-dependent regulatory framework will not fulfil the requirements of this Draft Law in relation to how it stands vis-à-vis EU legal framework.
- National security considerations may provide an acceptable case for exemption/exception to the data privacy framework, which is understandable for Turkey that is currently dealing with a number of external and internal security deficiencies. However, the broad and generous application of the issue of 'national security' on cases of data privacy and security will likely produce more problems that it resolves, as evidenced by the latest US – EU Data Protection Agreement. Excessive securitization of data privacy from the perspective of state agencies will render the proposed law fundamentally problematic and will likely create more problems on data sharing with the EU.
- The risk is that after reviewing this legislation, the EU may still consider Turkey as a safe country for the transfer of personal data. This would endanger the fulfillment of a key condition for the lifting of Schengen visas by October 2016.

- It would continue to hinder cooperation between the relevant Turkish agencies and EUROPOL and EUROJUST.
- But in addition it would create uncertainties for domestic as well as international companies that until now were able to engage in cross border transfers of personal data.