PAKISTAN'S
INTERNET
LANDSCAPE
2018

A REPORT BY BYTES FOR ALL, PAKISTAN
TABLE OF CONTENTS

06  INTERNET ACCESS
15  GOVERNANCE AND CRIME
23  BLASPHEMY
30  CHILD PORNOGRAPHY
36  CYBERCRIME
40  DATA PROTECTION AND PRIVACY
45  CENSORSHIP AND MEDIA
52  GENERAL ELECTIONS
58  FAKE NEWS
66  FIN-TECH AND BRANCHLESS BANKING
73  E-COMMERCE
PREFACE

The fourth edition of “Internet Landscape of Pakistan” is an exhaustive mapping of the digital trends that not only impact citizens’ social, economic and political rights, but also determines how responsive and efficient the government is in addressing peoples’ problems. This report, we hope, would be useful for media professionals, policy makers, civil society, academia, UN special mandate holders and International development partners.

The report comes at a time when Pakistan, like many other countries in Asia specifically, is witnessing a tense struggle between a vibrant civil society and an oppressive, coercive and controlling polity. Over the year, since the last edition of this report was published, Pakistan has faced far greater control over free expression, increased censorship, secrecy of public policy decision-making, and violation of fundamental freedoms of citizens.

It is noteworthy that since 2013, when the first edition of Internet Landscape of Pakistan came out, the usage of internet by the state and citizenry has increased manifold. Almost all organs of the state are visibly more concerned about what is said on the internet about them and of the services they deliver to the public.

Civil society has progressed tremendously in using the internet to highlight issues, to advocate legislative and political reforms, to sensitize people on complex issues concerning social justice and to gather mass support for human rights causes. However, just as civil society has adopted creative ways for expression through the internet, the state has also become more inventive in controlling opinion.

This report not only maps the trends in existing usage of the internet by all these stakeholders, but also dilates upon the possibilities of further innovation to not only bolster freedom of information and expression, but also to provide insight as to how the state could improve governance and service delivery to people. This also carries valuable information for tech start-ups and digital innovation projects undertaken by social entrepreneurs.

This particular study is another demonstration of the commitment of Bytes for All to create a level playing field for all segments of society by ending the digital divide through inspiring a positive change in digital trends. On behalf of Bytes for All, I’m grateful to Mr. Jahanzaib Haque – one of Pakistan’s top professionals in digital media, and lead researcher – for authoring this report and coordinating with his associates to deliver this in-depth study. This year, our research team has also gathered input from subject specialists of different fields to provide greater context.

I also take this opportunity to appreciate Mr. Shahzad Ahmad, Country Director Bytes for All, for initiating this series, providing leadership to the project and mobilizing resources for this important initiative. I offer my gratitude to the entire team of professionals at Bytes for All, who supported the process and worked out logistics involved in the study. Finally, Bytes for All is indebted to all the international and national partners whose timely and generous support was instrumental in the publishing of this report.

With this, I offer our work to all of you for your reading pleasure. I hope this proves useful for your endeavors.

Marvi Sirmed
Chairperson of the Board
This year’s Internet Landscape report has captured a wider array of developments in the online space, and an equally wide range of results, ranging from poor to positive.

Overall internet penetration continues to increase, bolstered largely by mobile phones with internet connections; the regulatory body Pakistan Telecommunications Authority reports a total of 62 million 3G/4G subscribers form 29.55% of penetration. However, the fundamental challenge of the urban-rural, socio-economic divide remains in place, and in relation to other countries, Pakistan is low on lists such as the Economic Intelligence Unit’s Inclusive Internet Index 2018, which ranks the country at 68th amongst 86 countries. Cellular network suspensions have also continued in the name of national security, exacerbating the situation.

The state has made some effort to improve governance through the internet with particular strides by law enforcement agencies. Most efforts, while positive, are early initiatives whose adoption and success can only be assessed at a later date.

Regarding blasphemy online, a new fear has emerged. The possible addition of clauses specific to blasphemy in the already controversial Prevention of Electronic Crimes Act could result in serious harm both online and offline through misuse and abuse of the laws. False blasphemy accusations and the targeting of minorities were seen this year – an ongoing trend that may spiral out of control. Some strides were made to curb child pornography, with awareness raised and an increasing number of arrests carried out. The extent to which this crime exists across the country is worrying however; it is likely that the finds of 2018 are just the tip of the iceberg. Questions about inadequate policies and laws governing child pornography and the abuse of children persist. A similar situation exists with regards to cybercrime, where women and children were targets in the vast majority of reported cases.

There were a number of large-scale hacks, including ride-hailing app Careem and Bank Islami, that exposed grave threats to data and privacy in Pakistan. The general elections also saw citizen data being shared widely for political purposes, raising questions about existing laws and policies. Through case studies, it is also clear that the state and/or other actors have continued surveillance of activists and journalists, resulting in intimidation and harassment. The situation is alarming, with freedom of speech negatively impacted this year. Traditional media and associated journalists have found themselves to be the targets of intimidation, harassment, violence and even monetary losses, resulting in self censorship across all media, including online – a space once considered the alternative to express ideas that could not be shared elsewhere. The state and the military are reportedly complicit in this effort. The planned establishment of a new regulatory body for the media appears to be a continuation of this crackdown on speech. Facebook and Twitter have both assisted the state on this front, to varying degrees.

Part of the reason for this concerning trend can be linked to the general elections that were held in July, and the new government that came into place. The elections themselves saw all political parties compete fiercely to win votes through the online space. This also resulted in a large volume of hate speech and fake news targeting political opponents. Due in large part to social media, and specifically WhatsApp and Facebook, fake news is an ever-growing challenge in the country.

One positive development was the launch of a portal to allow overseas Pakistanis to vote in the elections. However, participation in the by-elections was extremely low, raising questions about the exercise. There were also concerns about rigging through the system.

Perhaps the biggest, and arguably most positive, developments came on the fin-tech/online banking and e-commerce front. While numerous, basic challenges face the industry, the potential of the online space has become clear, with sentiments largely positive following major global players like retail and e-commerce giant Ali Baba entering the market.

In summary, despite taking a few steps forward, at the macro-level the country remains without a cohesive, progressive and all-encompassing approach to the internet and the implications of living in a digitized world.
The latest research and indicators paint a mixed picture when it comes to internet access and use in Pakistan.

On the one hand, the country’s mass adoption of mobile phones with internet services has bolstered overall penetration stats. At the same time, many challenges persist when it comes to a large gender gap in access, urban vs rural adoption, general knowledge of the internet and its uses, investment in Information and Communications Technology (ICT) that would enable growth, the setup of infrastructure in remote areas and more.

The country remains extremely low ranked on multiple international scorecards when it comes to internet access, and systemic issues such as suspending cellular networks for security reasons continue to impede progress.
PTA TELECOM INDICATORS

154 million
Cellular Subscribers
73.85% Teledensity

62 million
3G/4G Subscribers
29.55% Penetration

3 million
Basic Telephony Subscribers
1.30% Teledensity

64 million
Broadband Subscribers
30.59% Penetration

*Figures are updated as on December 2018

BROADBAND SUBSCRIBERS BY TECHNOLOGY

<table>
<thead>
<tr>
<th>Technology</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile BB</td>
<td>0.51%</td>
</tr>
<tr>
<td>EvDO</td>
<td>0.13%</td>
</tr>
<tr>
<td>FTTH</td>
<td>0.10%</td>
</tr>
<tr>
<td>WiMax</td>
<td>0.09%</td>
</tr>
<tr>
<td>HFC</td>
<td>2.52%</td>
</tr>
<tr>
<td>DSL</td>
<td>0.04%</td>
</tr>
<tr>
<td>3G 4G LTE</td>
<td>96.61%</td>
</tr>
</tbody>
</table>

*Figures are updated as on November 2018

CELLULAR MARKET SHARE

<table>
<thead>
<tr>
<th>Operator</th>
<th>Market Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telenor</td>
<td>28.46%</td>
</tr>
<tr>
<td>CMPAK (Zong)</td>
<td>21.01%</td>
</tr>
<tr>
<td>PTML (Ufone)</td>
<td>14.02%</td>
</tr>
<tr>
<td>PMCL (Jazz)</td>
<td>36.51%</td>
</tr>
</tbody>
</table>

*Figures are updated as on November 2018

Pakistan is ranked at 68th amongst 86 countries when it comes to internet penetration. Pakistan ranks the lowest worldwide vis-a-vis gender access parity, with a 266 percent gap in internet access rates and a 121.2 percent gap in mobile ownership in favor of men.

THE ECONOMIST INTELLIGENCE UNIT’S INCLUSIVE INTERNET INDEX OF 2018
ACCESS AND USE SURVEY

A comprehensive survey on ‘ICT access and use in Pakistan and the Global South’ was published this year by After Access, an ICT policy and regulation think tank. The nationally representative survey had a 95% confidence level with a +/- 3.3 margin of error. Its key findings included:

37% of those aged 15-65 know of/have heard of the internet

53% of internet users came online less than a year before survey

17% of population use internet, 14% on social media

INTERNET AND SOCIAL MEDIA USE

(\% of aged 15-65 population)

INTERNET ACCESS

<table>
<thead>
<tr>
<th>Country</th>
<th>% of aged 15-65 population</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cambodia</td>
<td>34%</td>
</tr>
<tr>
<td>India</td>
<td>15%</td>
</tr>
<tr>
<td>Nigeria</td>
<td>14%</td>
</tr>
<tr>
<td>Pakistan</td>
<td>17%</td>
</tr>
<tr>
<td>Ghana</td>
<td>26%</td>
</tr>
<tr>
<td>Myanmar</td>
<td>21%</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>13%</td>
</tr>
<tr>
<td>Guatemala</td>
<td>62%</td>
</tr>
</tbody>
</table>

INTERNET USE

<table>
<thead>
<tr>
<th>Country</th>
<th>% of aged 15-65 population</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cambodia</td>
<td>36%</td>
</tr>
<tr>
<td>India</td>
<td>30%</td>
</tr>
<tr>
<td>Nigeria</td>
<td>20%</td>
</tr>
<tr>
<td>Pakistan</td>
<td>17%</td>
</tr>
<tr>
<td>Ghana</td>
<td>29%</td>
</tr>
<tr>
<td>Myanmar</td>
<td>30%</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>13%</td>
</tr>
<tr>
<td>Guatemala</td>
<td>65%</td>
</tr>
</tbody>
</table>


21\% of males online, versus only 12\% of females

Line represents gender gap (\%)

<table>
<thead>
<tr>
<th>Country</th>
<th>Male</th>
<th>Female</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>57%</td>
<td>11%</td>
</tr>
<tr>
<td>Nigeria</td>
<td>46%</td>
<td>21%</td>
</tr>
<tr>
<td>Pakistan</td>
<td>43%</td>
<td>21%</td>
</tr>
<tr>
<td>Ghana</td>
<td>33%</td>
<td>22%</td>
</tr>
<tr>
<td>Myanmar</td>
<td>37%</td>
<td>24%</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>62%</td>
<td>7%</td>
</tr>
</tbody>
</table>
INTERNET ACCESS

AVERAGE DOWNLOAD SPEED (MBPS), URBAN-RURAL

- Cambodia: 1.95 Mbps (urban), 2.62 Mbps (rural)
- Nepal: 0.52 Mbps (urban), 1.6 Mbps (rural)
- Pakistan: 1.72 Mbps (urban), 2.84 Mbps (rural)
- Bangladesh: 1.88 Mbps (urban), 1.54 Mbps (rural)
- India: 2.04 Mbps (urban), 4.12 Mbps (rural)

2.84 Mbps is avg download speed in urban areas; 1.72 in rural

57% of population own a mobile phone

5% less likely to own a mobile if living in rural areas

MOBILE PHONE OWNERSHIP
(% of aged 15-65 mobile phone owners)

- Guatemala: 30% (basic), 14% (feature), 57% (smart)
- India: 55% (basic), 16% (feature), 23% (smart)
- Nigeria: 31% (basic), 46% (feature), 23% (smart)
- Pakistan: 53% (basic), 25% (feature), 22% (smart)
- Ghana: 52% (basic), 14% (feature), 35% (smart)
- Bangladesh: 40% (basic), 37% (feature), 24% (smart)
- Cambodia: 42% (basic), 10% (feature), 48% (smart)

343 rupees is the avg spent monthly on voice+data packages

37% less likely to own a mobile if female

22% use smart phones as primary device, 53% use phones with no internet
**SURGE ON THE MOBILE INTERNET FRONT**

Research body GSMA Intelligence published a key finding in its Mobile Trends Report this year: Five countries will account for 50% of the growth of 1.6 billion new mobile internet users between now and 2025, with Pakistan being one of those countries. China and India will drive most of the growth, with Indonesia, Nigeria and Pakistan accounting for over 50 million users each.²

The report also highlighted that fixed broadband is negligible in these countries, and as a consequence, the next internet generation will be mobile only, rather than mobile first. It also cited a continued decline in prices of smartphones (driven by cheap, Chinese phones) and a reduction in mobile data cost as factors for this rise.

**MONTHLY DATA BUNDLE COSTS IN MAJOR EMERGING MARKETS**

<table>
<thead>
<tr>
<th>Tariff as percentage of monthly income, medium bundle</th>
<th>Source: GSMA Intelligence, Tarifica</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0%</td>
<td></td>
</tr>
<tr>
<td>0.5%</td>
<td></td>
</tr>
<tr>
<td>1.0%</td>
<td></td>
</tr>
<tr>
<td>1.5%</td>
<td></td>
</tr>
<tr>
<td>2.0%</td>
<td></td>
</tr>
<tr>
<td>2.5%</td>
<td></td>
</tr>
<tr>
<td>3.0%</td>
<td></td>
</tr>
<tr>
<td>3.5%</td>
<td></td>
</tr>
<tr>
<td>4.0%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Country</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nigeria</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pakistan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mexico</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kenya</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>India</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indonesia</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**AT THE BOTTOM**

Huawei’s Global Connectivity Index 2018 ranked Pakistan at a low 77 out of 79 countries on the ICT front. Only Bangladesh and Ethiopia fared worse.

The country scored 25/100 on a host of indicators ranging from ICT laws to 4G coverage, fiber optic, internet bandwidth, investment into ICT, telecom, big data, IoT and more. As shared in the country profile: “Pakistan is not an information technology powerhouse, it scores at 2 for ICT investment while average score for these 80 countries is average at 4.4 this year. Its Internet penetration remains low, with the volume of mobile broadband services exceeding the fixed broadband sector of the market. Smartphone penetration rate continue to go upward and users experience in terms of FBB affordability, cloud migration and broadband download speed had improved for the year.

Broadband access in Pakistan in particular remains limited, but this sector of the market was finally starting to expand, having been given a massive boost with the arrival of mobile broadband. The country has been pursuing an aggressive IT policy, aimed at boosting Pakistan’s drive for economic modernization. Of special significance has been the administration’s provisioning of e-government services.”


ACCESS TO REMOTE AREAS

While urban centers have for some years seen access to increasing high speed internet available in multiple forms from fiber optic connections to mobile 4G, the challenge of providing meaningful access in remote areas of the country remains.

TELCOS DO THE WORK

One of the primary programs the state has adopted and maintained across 2018 to tackle the issue is the Universal Service Fund (USF), which operates under the Ministry of Information Technology. The project allows for telecom services to be provided to remote areas which may not be lucrative for telcos otherwise.

So far, through 3G/4G services, the USF has provided internet access to 5,896 Mauzas, while new contracts would extend services to Khyber, Mohmand and DI Khan at a cost of Rs 3.5 billion, servicing over four million people in 1,187 Mauzas.

Utilising USF funds, the Ministry of IT also launched the Broadband for Sustainable Development Programme this year, aimed at providing telecom services to chronically underserved parts of the war-torn Federally Administered Tribal Areas (FATA). An agreement was sign to provide broadband internet to “accelerate socio-economic development of 5,896 villages of FATA.”

One telco, Zong, also launched operations in the fast-developing port city of Gwadar, which is seen as critical to CPEC. This development follows a report that noted slow internet has hampered development and operations in Gwadar. As stated in the report, Dostain Khan Jamaldini, chairman of the Gwadar Port Authority shared that the customs authority’s online system was “riddled by delays due to a slow internet connection and an alternative wireless system installed by the Chinese too is facing bandwidth problems.”

ROAD TO PROGRESS

Rizwan Mir, CEO, Universal Service Fund outlined challenges and opportunities for growth in his article “Current state of broadband in Pakistan, way forward”.4

01 The deployment of mobile networks needs to speed up.
02 Mobile broadband is not scalable – the industry is relying too much on it.
03 Wired broadband needs to be expanded urgently.
04 Right of Way for laying fiber needs effective tariff and policies.
05 Heavy taxation on the telecom sector needs to be eased.
06 Government grants/subsidies are critical for broadband penetration to underserved areas.

“We note with grave concern that not only Fata region but large parts of Balochistan, Azad Jammu and Kashmir, Gilgit-Baltistan and most remote areas are still deprived of real Internet access in the country. It’s also worrisome that the government preferred to use Universal Service Fund (USF) for debt servicing rather than providing good quality access to its citizens. This deprivation should end immediately.”

BYTES FOR ALL, PAKISTAN

---

In one unusual development, Zong was prevented by the courts from launching 3G/4G services in the sensitive Gilgit-Baltistan region, which has for years seen poor to non-existent internet access. The PTA’s decision to allow private operators into the area was stayed in favour of continued service by the Special Communications Organisation (SCO), which holds a monopoly in GB and Azad and Jammu Kashmir (AJK). The petition had been filed by the SCO itself, which is the telecommunication wing of the Pakistan army.\(^\text{10}\)

Security concerns have resulted in complete blockages of internet access in multiple sensitive regions, with some of the blocks having been in place for years. For example, 3G internet services had been suspended for over a year in Chagai, Pishin, Panjgoor, Killa Abdullah resulting in protests this year. One political worker shared that, “Only DSL is working in Dalbandin. But its speed is so slow that it is of no use.”\(^\text{11}\)

**CHINA TO THE RESCUE**

Potentially the biggest game changer in terms of internet access in remote areas has come from China, with the inauguration of the Pak-China Optical Fiber Cable (OFC), a CPEC project which forms the first land-based communication link between Pakistan and China.

Laid out across the Gilgit-Baltistan region, the 820-kilometre-long underground cable runs from Rawalpindi to Khunjerab and then also continues as a 172-km aerial link from Karimabad to Khunjerab.\(^\text{12}\) The OFC cost $44 million to developed, backed by a 85% concessionary loan from the Exim Bank of China. The project is owned by the military-run SCO, while its engineering, procurement and construction (EPC) contractor is Huawei.\(^\text{13}\)

The cable is expected to extend down to Gwadar in the long term, providing further connectivity to far flung areas along the western border and Balochistan.\(^\text{14}\)

Aside from the OFC, China is also working with Pakistan to set up a new submarine cable with landing routes in Karachi and Gwadar, further ensuring faster connections and lowering the likelihood of a major net breakdown in both urban and rural areas. Named **PEACE** (Pakistan East Africa Cable Express) the project will be built by Huawei Marine, funded by Tropic Science Co Ltd and managed by the telecom giant PCCW Global. Huawei claims the cable’s deployment has started this year and will be complete by the end of 2019.\(^\text{15}\)

---


### Timeline of Mobile Network Suspensions

<table>
<thead>
<tr>
<th>Date</th>
<th>Reason</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 23</td>
<td>Pakistan Day</td>
<td>Islamabad</td>
</tr>
<tr>
<td>July 13</td>
<td>Nawaz Sharif, Maryam Nawaz arrested</td>
<td>Lahore</td>
</tr>
<tr>
<td>July 21-31</td>
<td>General elections</td>
<td>Parts of Balochistan</td>
</tr>
<tr>
<td>September 19-21</td>
<td>Muharram processions</td>
<td>Many parts of Pakistan</td>
</tr>
<tr>
<td>October 30</td>
<td>Chehlum of Hazrat Imam Hussain (RA)</td>
<td>Many parts of Pakistan</td>
</tr>
<tr>
<td>November 2</td>
<td>Protests after Aasia blasphemy case verdict</td>
<td>Major cities</td>
</tr>
<tr>
<td>November 21</td>
<td>Eid celebrations</td>
<td>Many parts of Pakistan</td>
</tr>
</tbody>
</table>

### The Countries Shutting Down the Internet the Most

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of Internet Shutdowns</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>154</td>
</tr>
<tr>
<td>Pakistan</td>
<td>19</td>
</tr>
<tr>
<td>Iraq</td>
<td>8</td>
</tr>
<tr>
<td>Syria</td>
<td>8</td>
</tr>
<tr>
<td>Turkey</td>
<td>7</td>
</tr>
<tr>
<td>D.R. Congo</td>
<td>5</td>
</tr>
<tr>
<td>Ethiopia</td>
<td>5</td>
</tr>
<tr>
<td>Iran</td>
<td>4</td>
</tr>
<tr>
<td>Chad</td>
<td>3</td>
</tr>
<tr>
<td>Egypt</td>
<td>3</td>
</tr>
</tbody>
</table>

Source: Access Now via Vice News

*An internet shutdown occurs when someone (usually the government) intentionally disrupts the internet of mobile apps to control what people say or do.

### Did You Know?

In February, the Islamabad High Court had declared it illegal to suspend mobile phone services in the name of security.
Comment

The e-governance potential

Khurram Saleem, Manager Operational Excellence at National ICT R&D Fund

E-Governance is about applying information and communication technology to all aspects of a government’s business where it makes sense to improve efficiency and effectiveness in the achievement of policy and program outcomes. There are many federal, provincial and local eGov initiatives in Pakistan, but the current approach is rife with problems such as:

1. Increase in processing steps
2. Difficulty of use
3. Higher cost
4. Lack of accountability
As a result, Pakistan’s UN eGov 2018 ranking is low. Several hundred federal, provincial and local government agencies have provided some sort of web services so far, though most are informational and interactive, with a few transactional ones, and one collaborative service i.e. Digiskills.pk

The government is working on introducing eServices on all three broad levels of G2G, G2B and G2C.

At the G2G level the government is working to replace the current physical paper based file system in the all ministries with an eOffice system, which has been developed and is being implemented across all ministries. A lot of government data is now available in digital format.

The introduction of digital services to facilitate the lives of all stakeholders is imperative and the government is cognizant of the benefits that a documented formal economy entails. Gov.uk as an example is expected to save $50 billion a year. In UAE almost $1.5 billion of government costs are being saved through reduced paper, travel, and transaction time. India Stack, with mobile broadband and Innovation/IT boost, is projected as a $1 trillion a year opportunity by 2030. Bill Gates believes this will allow India to vault over USA. Estonia X-Road places 99% of government services online, with 52,000 organization users, 800 years working time saved, and dealing with 500 million queries annually.

Based on the above, Government as a Platform (GaaP) – similar to Gov.uk and Xroads Estonia – needs to be setup so that government organizations can deliver next generation public services. It will delight citizens, ease business, expand the formal economy, boost the IT industry and provide transparent, accountable and efficient governance.

A Public private partnership approach can be used to address the problem that is tech agnostic and not hostage to any vendor. It will create a roadmap that manages risk and builds incrementally and can carry along different levels of governance and officials.

This platform will fundamentally change the way the government operates and its very relationship with the citizens. It can establish the state as a big, daring entrepreneur, innovator and risk capital provider across industrial value chains.

A lot of money is required to initiate large-scale automation of government services, but it is imperative in order to succeed in the drive for a knowledge economy and also the ease of doing business rating, which to-date has a dismal standing in Pakistan.
Governance through the internet, and in particular efforts to tackle crime, intermittently made headlines with multiple initiatives large and small green-lighted, experimented with or implemented. While not an exhaustive list, a set of projects and achievements by various branches of government are listed below.

Note: Other initiatives are also mentioned in various sections of this report.

**BUSINESS AND ECONOMY**

**PAY TAXES ONLINE**

Through the efforts of FBR and SBP, a new online tax collection system was launched that allowed payment of taxes and duties through internet banking accounts or ATMs. Connected to the 1Link Biller module, the 24-hour system would allow payments of income tax, sales tax, customs duty and federal excise duty.¹

In order to make payments, users would have to generate a payment slip ID by first filing their details into the FBR IRIS system and Customs WeBOC. This ID would then be inputted online/at an ATM to display details for completing a payment.

IRIS-ADX

The Federal Board of Revenue (FBR) introduced the Iris-ADX (Asynchronous Data exchange) app which allowed taxpayers to prepare their tax data offline prior to submission. This app was created to solve connectivity issues in uploading data, particularly for large taxpayers. The Iris-ADX will also allow offline preparation of income tax returns and statements.²

PAK-CINA EDI

In order to facilitate quick sharing of import and export data, the Exchange of Data Information (EDI) between Pakistan and China was established as a digital solution to the issue of under-invoicing. According to a news report, Islamabad was facing under-invoicing between $4-6 billion annually. An FBR official said an added benefit would be a 'multiplier effect' on taxation along with greater tax collection.³

OECD INFORMATION SHARING

A digital system was set up at FBR (along with six automatic exchanges of information (AEOI) zones) to allow for the sharing of financial information about bank accounts of non-residents between Pakistan and the Organisation for Economic Cooperation and Development (OECD) nations. The data-sharing comes under a multilateral tax convention, including the closing of AEOI zones. The data will be shared for each year with member countries, and reciprocated with Pakistan's information requests.⁴

**NATIONAL SINGLE WINDOW FOR CUSTOMS**

Late in the year, the government approved the development of a digital trade hub to allow for the speedy clearance of cross-border consignments. The project, dubbed 'National Single Window' (NSW), is estimated to cost $163 million and will be led by Federal Board of Revenue’s (FBR) Customs Wing.

Finance Minister Asad Umar shared that the system would improve Pakistan's electronic logistics platform, with completion set for 2023. NSW aims to link all cross border trade regulatory authorities on a single platform to improve transparency and predictability in imports and exports while cutting down costs/time, both for public and private sectors. He stated that the system would improve efficiency of sea and airports as well.⁵

The FBR NSW Programme Director Imran Mohmand claimed, “The new system will cut annual import and export cost by $800 million if we manage to improve the cross-border trading system by 3%...the benefit of cost reduction will go to the private sector.” He added that traders would be able to file trade documents at one place instead of the current 42 agencies that include banks, insurance, port, customs and others.⁶


Online terrorism, and where Pakistan stands

Norbert Almeida, Security Advisor

Online extremism in Pakistan will not be curbed by simply blocking a few sites or reporting a few accounts. Block and control messaging, but given that the state keeps changing what it considers extremism and whom it considers a terrorist, such actions will always be challenged and lack support. To be very clear, the state must first own its policy and then apply it consistently, or face criticism and failure.

Bear in mind, extremists/terrorists will always find ways to indoctrinate others, and the anonymity of the Internet makes it easy for them to get away with it. Therefore, cyberspace poses two major challenges; the struggle to keep up with the pace of technology, and the broader issue of online users identifying with extremist viewpoints.

This particular battle is not online, it is offline. When people have reasons to accept an extremist viewpoint readily, it doesn’t matter how the message is conveyed to them. The state must focus on eliminating those factors, whether that is through education, job creation or other means. In viewing this issue as an online problem, we will simply be tackling the outcome, and not the cause.

Muhammad Amir Rana, Director, Pakistan Institute for Peace Studies

The online space is extremely dangerous for Pakistan’s youth as they are exposed to messages of hatred and extremism from a multitude of sources. Militants and their supporters aren’t the only ones spreading hate; the issue is so rampant there are many who spread such information online without being a part of such groups. An absence of counter messages further compounds the problem. All this results in the spread of a culture of hatred and violence aimed at leading people to rebellion against state – one of the main agendas of the terrorists.

Aside from spreading their message, extremists and terrorists systemically use online spaces to recruit, including through the dark web, which authorities find difficult to monitor. In many instances, Daesh and Al-Qaeda were found involved in recruiting in Pakistan through the internet. In the past few years, law enforcement agencies have busted several such small cells of individuals who were radicalized online and recruited by Daesh.

The government is not doing enough, and the disseminators of hatred and extremism are far ahead in propagating their message. The state’s responses are scattered and exclusive. There is no doubt that FIA and PTA, as well as NACTA are busy in countering extremists’ online campaigns but they still have a long way to go.

There were also reports that the government is developing a National Cyber Terrorism Security Investigation Agency to counter online hate speech and messages of extremism and violence, but on the whole the militants groups, particularly religious ones, are operating with relative impunity online using different names and tactics. There is a need to focus more on soft approaches to countering violent extremism and terrorism, which will ultimately counter online radicalism.
CRIME/TERRORISM

WELFARE EYE, LOCAL EYE, 111 INTELLIGENCE

After a launch in Punjab, followed by adoption in Sindh, local IT projects Welfare Eye, Local Eye and 111 Intelligence were requested by the Balochistan police force, indicating further success of the initiatives.

Developed by Punjab Information Technology Board with the Punjab Police, Welfare Eye is an application that connects families of martyred police officers make requests for assistance; Local Eye connects the public directly with police officers; 111 Intelligence allows different security forces to quickly pass on intelligence related to crime and terrorism.

As noted by the AIG Information Technology Balochistan Police, “These IT programmes have proved to be a success story in providing sustainable relief to the people, fighting outlaws and anti-state elements and uplifting morale of force by ensuring different welfare measures.”

PUNJAB POLICE TOOLKIT

The Punjab Police created an investigative Android mobile app that allows officers to access/verify data related to cases on-the-fly. The ‘Punjab Police Toolkit’ provides access to data of all 36 districts of Punjab, and was developed by Punjab Information Technology Board (PITB) for internal communication only. Data sets included phone numbers, driving license, criminal records, vehicle ownership, stolen vehicles, wanted persons, FIRs and more. It also provides data of work carried out by police officers on a daily basis, thus creating a system of accountability.

A CYBERCRIME PORTAL FOR SINDH

In a first for any province, the Sindh chapter of the of Federal Investigation Agency (FIA) launched a website, www.fiacybercrimesindh.com.pk, to register complaints. The site could register complaints in English, Urdu or Sindhi to facilitate the public better. The FIA claimed that complaints registered through the portal would be addressed within 48 hours, or contact would be made within minutes if the case was urgent.

CYBERCRIME STATS

January-August 2018

4,000 complaints

With only 10 officials working on cases

90% of cybercrime victims are women/minor girls
90% of crimes committed on Facebook/WhatsApp
70% of cases involve pornographic content
30-35 days before Facebook responds to assist
6-9 months before cases are resolved

90% of crimes committed on Facebook/ WhatsApp
36 of 75

Pakistani banned outfits are active on social media

Source: FIA

DID YOU KNOW?

FIA cybercrime performance report Q1, 2018

THE SURF SAFE PORTAL

The National Counter Terrorism Authority (NACTA) developed the Surf Safe portal for citizens to anonymously report online extremism and abuse. The broad objective was to counter extremism in cyberspace – an implementation of the National Action Plan (NAP) against terrorism. A supporting mobile app was also developed by NACtA as well.
GOVERNANCE AND CRIME

**Pakistani Citizens' Portal**
The Pakistan Citizens’ Portal was a high-profile project that was launched by Prime Minister Imran Khan itself. The platform, an initiative of the Prime Minister Performance Delivery Unit (PMDU), was developed to allow citizens to register complaints or provide feedback and suggestions on the working of the government in all areas. It was cited to be a ‘first’ in the country’s history as it connected to about 4,000 government offices.¹⁴

As of end of December, the Google store indicated the Android app had been installed over 500,000 times.¹⁵ At the end of the year, Prime Minister Imran Khan shared that the government had resolved over 100,000 complaints registered through the portal.¹⁶

**Pakistan Post App**
Pakistan Post launched a mobile app to allow users to track their parcels. The system would require an RFID sticker to be added to a parcel for tracking at a cost of Rs9.¹⁷ The app also allows users to register complaints, explore postal services, tariff, post codes, locate a post office and contact Pakistan Post.¹⁸

**Pakistan Railways Mobile App**
In December, the Pakistan Railways announced it would be launching a mobile app for customers looking to purchase tickets, check train schedules and locations of trains. The project involves the installation of trackers on all trains to update customers on locations, and even real-time train speed. The app would be replacing the old system of phone enquiry through 117.¹⁹

**Hara Bhara Pakistan App**
The Sindh government developed the ‘Hara Bhara Pakistan’ mobile app that allows users to geo-tag photos of trees being planted to help keep track of location and quantity of new trees.

The environmental initiative was aimed at creating awareness about the need for tree plantation, and to encourage planting at a mass-scale.²⁰

---

**PTI’s 14 Points for Digital Pakistan**

01 $2 billion set aside for National digital transformations & provision of different services to citizens through mobile.

02 Using technology to open government data to increase transparency

03 IT education of 50,000 students

04 Establishment of 120 new campuses to produce 100,000 technology graduates/year

05 Mathematics and Science teacher training and certification program

06 Five new major technology clusters (Special Economic Zones)

07 A focus will be on creating enabling environment for start-ups and entrepreneurs.

08 50,000 call center seats available on a turn-key basis

09 One window operation to register a new company

10 A global PR campaign involving expat community

11 Visa issuance on green passport for Businessmen and professionals

12 Simplification of processes for foreign ownership of companies

13 Public-Private Partnership on projects

14 Target will be set to increase the global ranking of Pakistan in ease of doing business

---


NATIONAL JOB PORTAL IN THE WORKS

A key meeting was held this year to finalise plans for the development of a National Job Portal and accompanying mobile app aimed at connecting job seekers with potential local/international employers across Pakistan. The mobile app would provide a separate GPS-based service allowing for quick hiring of skilled workers such as electricians, carpenters, painters, tailors etc. No timeline was provided for completion of the platform.²¹

NHA APP

The National Highway Authority (NHA) launched a mobile app as part of a right-to-information initiative, whereby users would be able to access details of the NHA’s projects.

Accessible information would include fiscal status of the ongoing and completed projects, source of funds, companies awarded contracts, physical/financial progress, toll rates, road safety guidelines, CPEC alignments, as well as two tools – Journey Planning and Interactive Maps – that help commuters plan trips.²²

ELEARN APP

On the education front, PITB launched a mobile app (also available as a web app), eLearn, that provides access to digitized Punjab textbooks for students from grades 6 to 12. The app, which was developed with the Punjab Curriculum & Textbook Board and the School Education Department, provided the books with additional interactive material such as video lectures, animations, simulations etc.

In total, the app provides access to 28 Science and Mathematics textbooks, 13,047 video lectures, 592 simulations, 2,100 minutes of audio and 1,830 animations.²³

THE DAESH ARREST

The arrest of suspected Daesh operative Imran, also known as Saif-ul-Islam Khilafati provided insight into how terrorists operate online. Picked up by the FIA in March, Imran was found to be operating over 50 pages on social media to recruit locals, largely college-going males, to the terror outfit.²⁸

During interrogations, he shared that his modus operandi included the use of proxies/VPN, temporary email accounts, communications app Telegram and accessing the dark web. He also alleged to have maintained contact with the global outfit through a WhatsApp group.²⁹

CYBERCRIME AGENCIES UPDATE

FIA was allowed to establish 15 cybercrime reporting centres across Pakistan; five in Punjab, three in Sindh, three in KP, two in Balochistan, one in Islamabad, one in Gilgit.²⁴

The government hoped to establish the National Cyber Terrorism Security Investigation Agency to tackle the issue of terrorism online. The Interior Ministry’s budget was to be increased by Rs100 million to establish the agency.²⁵

The National Center for Cyber Security was launched at Air University, Islamabad, aiming to secure cyberspace by becoming a hub of research and innovation. A BS in Cyber Security was also on offer for students. Additionally, a number of affiliated labs would be set up at other universities.²⁶

A new Cyber Patrolling Unit was proposed to be launched under the FIA. The project, estimated to cost Rs54.2 million, would compromise of a 40-member team tasked to monitor and investigate online cases.²⁷

---


Tackling crime through tech

Norbert Almeida, Security Advisor

There is absolutely no question that technology is assisting in fighting crime e.g. through crime reporting. However, where is the analysis and reporting around those cases that have been solved following reporting? Where is the awareness campaign around it? These technological solutions are only going to be effective when people see results. If you are a victim of a crime and report it and get a response you deem satisfactory you will talk about it.

When it comes to action and awareness, the passport office experience and ID card experience are superb examples, as is the digitization of many services in Punjab. It took major awareness supported by concrete actions by the state to lead us to a place where citizens will more often than not praise these services. Crime reporting will need to experience such a change for it to truly grow. Additionally, confidence must be built in users that there is no repercussion or negative consequence to reporting a case.

Muhammad Amir Rana, Director, Pakistan Institute for Peace Studies

Technological solutions to fighting crimes, such as the development of online apps, will first have to pass the tests of time and utility. At the moment it is too early to assess whether these initiatives are effective as there is no public data available to answer questions such as how many people use them, are they actually addressing their problems and concerns etc.

Such initiatives should hypothetically greatly help in fighting crime e.g. by connecting ordinary citizens to law enforcers, giving fast, easy access to online databases, register complaints etc. There is also reason to believe that digital tools will inject transparency in policing, law enforcement and justice; a radical change in the traditional culture that works on patronage and corruption. They may also uplift the morale of law enforcers.

There are many challenges though that will require concerted efforts to sustain and improve initiatives launched by the federal and provincial governments. For one, availability of trained human resource to effectively and professionally execute these initiatives will be a major challenge. Another will be expanding the outreach of the initiatives to communities and areas where there is less awareness/training in IT-related projects.

Winning people’s trust to use digital tools will be another challenge, mainly due to longstanding mistrust of the state’s service delivery apparatus. Finally, it will not be easy to convince different institutions to work together, especially in terms of intelligence and information sharing.
Social media has proven to be a double-edged sword. On the one hand, it has brought more voices, several critical of religious extremism, to the forefront. But at the same time it has also made it easier for people to be accused of blasphemy, and for the propagation of trends and fake news that can lead to dangerous outcomes. Most of Pakistan's mob violence still emanates out of incendiary khutbas by extremist clerics, but social media is becoming the new pulpit.

One response by the state has been to restrict access to content, but blocking something is never effective. Blasphemous material can easily be accessed. Viewpoints need to be debated and voted out from the marketplace of ideas. From the vantage point of those offended by blasphemous materials, it makes much more sense to vote down such content on e.g. video platforms and to strictly appeal to community standards.

Twitter has also been activated in terms of notifying users that they are violating Pakistan law in their posts. This is problematic because not only are some of the posts not in violation of Pakistani law, but some users who have been warned have no nexus with Pakistani territory, and are not even citizens. This amounts to a strange juridical ambiguity in jurisdiction. This will likely continue though, as the present government looks to ride populist waves.

More worryingly, a move to incorporate blasphemy into cybercrime laws is going to be a disaster of immense proportions. Not only will it not work, it will create an unnecessary furor. The cybercrime law i.e. Prevention of Electronic Crimes Act 2016 is problematic ab initio but introducing blasphemy sections into it and then leaving the application up to the will and whim of officials is going to be a new kind of threat.

So far, online activism to build counter narratives has not been as effective as efforts undertaken in an organised manner. Some voices, like that of Arafat Mazhar and his organization Engage Pakistan have effectively posed an organised challenge to the narrative that has found popular currency. It certainly can be more effective if it is done in an organised manner with the intention being not just to sermonise on freedom of speech but to come up with potent human rights, legal and religious arguments against blasphemy on the internet.
ONLINE BLASPHEMY: TIMELINE OF EVENTS

December 2018:  
**Christian brothers sentenced**

Qaiser and Amoon Ayub from Lahore were sentenced to hang by a district judge after being convicted of insulting the Prophet (PBUH) in articles and portraits posted on their website, United Christians Organisation of Pakistan, in August 2010. The complaint had been registered by a Muslim cleric from another district. The counsel for the two men said while they had started the website, they were not operating it at the time of the offence.¹

November 2018:  
**Expat booked for blasphemy**

An expatriate Pakistani living in Germany was booked after his “blasphemous” video went viral. A resident of Kathala Chenab village lodged the case against the suspect, who was a resident of the village and had settled in Germany many years ago. The applicant alleged that the suspect had aired his “blasphemous” video on a web-based television channel which was also available on YouTube and other social media sites. The complainant also demanded the extradition of the suspect from Germany and death penalty for him.²

August 2018:  
**Hindu boy arrested**

Police arrested a 19-year-old Hindu boy in Mirwah Gorchani for allegedly posting blasphemous content on social media. The complainant alleged that the boy had hurt religious sentiments of Muslims by posting ‘highly controversial’ material on Facebook. Locals claimed the suspect was upset after his sister Ganga (now Ayesha) had embraced Islam and married a Muslim man.³

February 2018:  
**FIR registered against Christian teenager**

An FIR for blasphemy was registered against an 18-year-old Christian boy in Shahdara, Punjab. The suspect was accused of circulating blasphemous content on social media leading to a protest against him outside his house. The mob ended the protest after an FIR was registered and police assured the crowd of taking action.⁵

---


January 2018:

**New Islamia College student kills principal**

A confession video of a student who killed his college principal for alleged blasphemy went viral online. In it, the student bragged about his actions and said he had no remorse. The principal had earlier expressed anger at the student for skipping college to attend the Faizabad sit-in which was planned in relation to suggested updates to the blasphemy laws.⁶

**LIFE & DEATH: PAKISTAN’S BLASPHEMY LAWS**

Pakistan’s Penal Code contains two offenses that result in life imprisonment or death for blasphemy.

<table>
<thead>
<tr>
<th>Offense</th>
<th>Description</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>295 - B</td>
<td>Defiling etc. of Holy Quran</td>
<td>Imprisonment for life</td>
</tr>
<tr>
<td>295 - C</td>
<td>Use of derogatory remarks etc. in respect of the Holy Prophet</td>
<td>Punished with death, or imprisonment for life, and also liable to fine</td>
</tr>
</tbody>
</table>

**STATE ACTION AND POLICY**

The government took two notable steps this year to address the issue of online blasphemy.

Early in the year, there was a proposal to introduce clauses in the cybercrime laws that would give equal punishment to blasphemers as well as false accusers of blasphemy. This effort was said to be in the name of curbing blasphemous actions committed online.⁷

A second step was to expand the Pakistan Telecommunication Authority’s (PTA) ability to block content, blasphemous or otherwise. The PTA had told the Islamabad High Court that it would look to install a ‘National Firewall’ to upgrade its technical capabilities. This expression of interest was later published, calling on companies that could help establish WMS through hardware, middleware, and software to allow PTA to identify and prevent access to content and sites deemed unlawful.⁸

---


RESPONSE TO BLASPHEMOUS CONTEST

The newly elected government was faced with a major challenge in the form of Dutch anti-Islam lawmaker Geert Wilders announcing a cartoon contest starting November that would feature blasphemous content. The contest would have inevitably led to protests and a violent reaction in Pakistan.

On its part, the Dutch government distanced itself from the contest, clarifying that Wilders was not a member of government, and this was not a government initiative. At the same time, Pakistan began a diplomatic drive that allegedly resulted in Wilders cancelling the contest due to "death threats and concerns other people could be put at risk". This was touted by the new government as a big achievement on its part.

TWITTER NOTICES

Micro-blogging site Twitter sent out numerous emails to journalists and activists both local and foreign across 2018, notifying them of "official correspondence" the company had received against tweets allegedly in violation of Pakistani law.

While unclear why this trend took off this year, a number of developments may have led to Twitter’s cooperation with authorities in Pakistan.

In July, the Islamabad High Court (IHC) has said that it could direct the Pakistan Telecom Authority (PTA) to block access to Twitter in Pakistan due to its failure to remove blasphemous content. This was followed by the PTA informing the Senate Standing Committee on Cabinet Secretariat that while Facebook, Youtube and other social media platforms complied with government requests to block content, Twitter did not do so. The regulatory authority had said it would implement the court order to block the site if Twitter did not respond to a final notice.

A few documented cases of notices sent out include:

**Anthony Furey**: (Journalist- Canadian) who posted blasphemous images in solidarity with cartoonists in retaliation to an ISIS inspired attack. Twitter correspondence stated the content was in violation of Pakistani law; Section 37 of PECA-2016, Section 295 B and Section 295 C of the Pakistan penal code.

**Ensaaf Haider**: (Wife of jailed Canadian-Saudi activist) who retweeted a woman in full veil with a caption that said "Repost if you’re against niqab".

**Imam Muhammad Tawhidi**: (Iranian-born Australian, Shia scholar) who tweeted "the police must investigate a mosque this terrorist attended for Friday prayers. Investigate the imam and the Friday sermon."

**Ahmed Waqas Goraya**: (Pakistani digital activist) received legal notices from Twitter stating he has violated Pakistani law; some of his tweets were allegedly restricted to the Pakistani audience.

**Gul Bukhari**: (Columnist) received a notice for her tweet in which she criticized the government’s lack of action against Tehreek-i-Labbaik Pakistan (TLP) Chief Khadim Hussain Rizvi.

**Imam Muhammad Tawhidi**

---


In January this year, a female Pakistani rights activist set a new precedent by seeking legal action against the person who accused her of violating the country’s anti-blasphemy laws.\(^{18}\)

Gulalai Ismail, founder of the Pakistan-based, nongovernment organization Aware Girls, was accused of insulting the religion of Islam, a charge she denied. Hamza Khan, 23, a student from Khyber Pakhtunkhwa province, started a social media campaign against Gulalai, accusing her of “insulting religion and Pashtun culture.” He seemingly was unhappy with her role as an activist. Khan, who claims to be the president of Mardan Youth Parliament, uploaded a 12-minute video on his Facebook page, November 20, 2017, in which he called for a mob to attack Gulalai for her alleged acts of blasphemy.

Fearing for her security, Gulalai filed a case against Khan on November 21 with the country’s Federal Investigation Agency (FIA), which led to Khan’s arrest.

While in previous years the issue of online pornography had been largely dominated by efforts by the state to block sites en masse, 2018 saw focus shift to child pornography being produced and disseminated online from within Pakistan.

**FAKE NEWS STIRS DEBATE**

Greater efforts on this front followed after the brutal rape and murder of Zainab Ansari, a six-year-old hailing from Kasur. The high-profile case that saw large-scale protests and a successful investigation was for some time connected to the online space after prominent anchorperson Shahid Masood claimed that the accused in the case was a member of a global network operating in the dark web, that was involved in the production and distribution of violent child pornography.

Interest in this angle was further heightened with debates in the media about the existence of the dark web; in one instance, a report in The Express Tribune cited an official from Federal Investigation Agency’s (FIA) Cyber Crime Unit alleging that incidents of child abuse across Pakistan clubbed with awareness about the dark web had led to over 1.3 million Pakistanis searching about the dark web in the space of only one week. The claims to Zainab’s murderer being connected to an online network proved to be untrue however, following a State Bank of Pakistan (SBP) investigation into the suspects bank accounts. Masood also backtracked from his statements.
Despite the above proving to be fake news, a number of cases emerged across the year that in fact did suggest that child pornography was being created locally and distributed online.

The most prominent case was the arrest of Saadat Amin, who was found to be holding more than 657,538 files (videos and pictures) related to child pornography.³ It was also uncovered that Amin was working with an international ring of child pornographers, earning at least 50,000 USD in the process.

The investigation revealed that Amin had filmed/photographs around 25 children between 8-14 years old. He would receive payments of 100-400 USD for the content through Western Union.⁴ He was later found guilty of the crime and sentenced to seven years imprisonment with a fine of Rs1.2 million.⁵

CASES ACROSS PAKISTAN

The arrest of Hafiz Muhammad Yusuf from Okara for making child pornography videos and blackmailing the victims.⁷

The arrest of one member of a four-member gang that was involved in filming children and distributing their videos online, while also extorting money from parents of the victims. The suspect was arrested from Gujar Khan after Interpol alerted Pakistan. Other members of the gang were based in Hong Kong and Dubai while one was untraceable in Pakistan.⁹

OTHER MAJOR UPDATES

The arrest of Taimur Maqsood in Satellite Town, Jhang for sharing child pornography online. The suspect was caught after a complaint was registered by National Child Exploitation Centre, Interpol in Ottawa, Canada, regarding his involvement with people from US, New Zealand, Australia and Canada.⁸

The arrest of four people including two engineers from Sargodha and Jhang, who were selling child porn online.⁶


A suspect was arrested from Abbottabad for his involvement in child pornography and illegal content was found on his gadgets. The tip-off came from Interpol, Spain.¹⁵

Based on these cases, in December the FIA announced a country-wide effort to crack down on child pornographers. The Director General of Federal Investigation Agency’s (FIA) Cyber Crimes Wing Capt (r) Muhammad Shoaib stated that he had ordered an inquiry into such cases and constituted a team to arrest those involved. He added that the major chunk of cases was based on tips from Interpol or foreign consulates/embassies.¹⁴

Following a complaint from Spain, a BBA student, Hamza was arrested from Karachi for making pornographic photos and videos of 10 children, aged 10-13. The student had used fake Facebook, Instagram and WhatsApp accounts to lure the children.¹² Hamza was operating a WhatsApp group with over 1,600 members who included victims and suspects.¹³


Also acting on a tip-off from Interpol Spain, the FIA arrested Waqar Ahmed, a resident of Tarbela, Haripur District in Khyber Paktunkhwa, for links with an international group of child pornographers. Pornographic material was found on his devices.¹⁰

Waqar Khan was arrested from his house in Mehran Colony in Ghazi Tehsil for selling pornographic videos of children.¹⁷
ISSUES WITH PUNISHMENT

With multiple arrests and growing awareness, a change in the existing cyber laws related to children was close to being passed.

In May, a parliamentary committee approved the Criminal Law (Amendment) Bill, 2018 which called for increasing punishments and fines for those convicted of child pornography. Maximum imprisonment was extended from seven years up to 14 years, while the fine was increased from Rs200,000 to Rs1 million.¹⁶ The bill, which covered many other aspects of cyber laws, was ultimately withdrawn by the new PTI government, citing a lack of scrutiny and secrecy in its formulation by the previous government.¹⁷

19A. Child pornography.- (l) Whoever intentionally produces, offers or makes available, distributes or transmits through an information system or procures for himself or for another person or without lawful justification possesses material in an information system, that visually depicts-

(a) a minor engaged in sexually explicit conduct;
(b) a person, appearing to be a minor engaged in sexually explicit conduct or
(c) realistic images representing a minor engaged in sexually explicit conduct; or
(d) discloses the identity of the minor. shall be punished with imprisonment for a term which may extend to seven years, or with fine which may extend to five million rupees or with both.

(2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (l) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances, including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

CHILD PORN CONVICTION SENTENCES

**Pakistan**
Imprisonment for up to 7 years

**India**
Imprisonment for up to 5 years

**USA**
Imprisonment for 15 - 30 years first time

**Japan**
Imprisonment for 5 years

**UK**
Imprisonment for 10 years

**Canada**
Imprisonment for 20 years

---


A long way to go on child pornography

Tahir Khilji, Founder and CEO of Vision.pk

An increase in reporting by the media in recent years has brought the issue of child pornography to the forefront, but this problem has always existed in our society; it is only now that we are aware of how widespread it is.

Following this raised awareness, more conversations need to be had, along with the introduction of a system of organic vigilance. We need to talk to children about body mapping, and explain what ‘safe’ and ‘unsafe’ online spaces are. So monitoring online habits and also creating streamlined awareness among children about body mapping is very important.

“If children have enough autonomy to have a presence online, then they should be aware of all the issues that come with online autonomy”

Social media can also be an effective tool to counter child pornography and child abuse perpetrated online. If the medium is being used to disseminate child pornography, the same medium could be used to counter it as well. This would require the combined efforts of the state and citizens.

Looking at the issue offline, a lot is lacking.

The existing laws are not adequate. For example, lawmakers are still not decided about the age of exposure. While boys are considered to be adults at 18, girls are not. This very framework needs to change. The problem is that the state wishes to work along convoluted definitions that fit an ‘Islamic Republic’ of Pakistan, resulting in this problem. As another example, the trafficking of children needs to be separately categorised and not framed as ‘human trafficking’ as their vulnerability should be recognised. The law has not touched on this. However, the Khyber-Pakhtunkhwa Child Protection and Welfare Act is fairly comprehensive, barring a few technical issues.

There also needs to be a lot more work done in understanding the language we use in reporting this issue. For example, the use of the word ‘ziyadti’ with infants is not comprehensive or even reflective of the issue of child sexual abuse. There is also the need to train law enforcing agencies e.g. in a workshop, it was found that officers believed that this issue is connected to lower income groups. That is not true; children are vulnerable in all income brackets.

There is a great need to raise awareness and sensitise policy makers to understand the related issue surrounding child sexual abuse such as child pornography. There needs to be a trusted course of action children and parents can take together.

Unfortunately, the state does not fully comprehend the problem, lacks capacity, and/or is wary of taking action based on existing data and reporting. Those in charge look upon data suspiciously, in some cases going as far as to order that data not be handed over to donors for fear of how it will be seen.

This suggests the state lacks commitment in these areas. It appears even the Human Rights Ministry has no sense of urgency to work on the issue. So as things stand, we have a state that spouts rhetoric and takes little concrete action.
All manner of cybercrimes saw an uptick this year, especially a sharp increase in the harassment and blackmailing of women. The FIA shared that its cybercrime unit had — as of October — conducted 2,295 inquiries, registered 255 cases and made 209 arrests in 2018; each an all-time high since the Prevention of Electronic Crimes Act (Peca), 2016 came into play.¹

While the government did make efforts to tackle the growing menace (See section: Governance and Crime), it appears likely that 2019 will see a further increase in cases.

### CYBERCRIME ARRESTS

<table>
<thead>
<tr>
<th>Year</th>
<th>Arrests</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>209</td>
</tr>
<tr>
<td>2017</td>
<td>160</td>
</tr>
<tr>
<td>2016</td>
<td>49</td>
</tr>
</tbody>
</table>

### CRIMES AGAINST WOMEN

#### SINGER BLACKMAILS GIRLS

Pashto singer Muneeba Shah was caught for blackmailing a girl via a fake social media account. Shah had allegedly been uploading pictures of girls on Facebook in order to blackmail them. A case was filed against the singer.²

#### SENTENCED TO 6 YEARS

Aamir Shams was sentenced to six years in prison for blackmailing girls on Facebook. He was also fined Rs400,000 with a penalty of further six months jail time if the sum was not paid.³

---


BLACKMAIL VIDEOS
Abdullah was arrested from a restaurant on Lahore’s Mall Road after a complaint was registered by the husband of a woman being blackmailed by the suspect. The complainant stated that Abdullah held inappropriate videos that he was using to blackmail his wife. Video data was recovered from the suspect’s mobile phone at the time of the arrest.⁴

90% of victims in cases reported to the Cybercrime circle in Lahore were women, and of that number 90% had their origins on Facebook.

EDITED PHOTOS
A suspect was arrested for blackmailing women he would entrap through matrimonial ads placed in daily newspapers. ‘Basharat’ would advertise himself as an army brigadier and ask women contacting him to share their photos, which he would then edit onto objectionable images and blackmail the women for money, with threats to share the doctored photos online. He also sexually assaulted some of the victims and videotaped them on forced visits to his home.⁵

65% of all cybercrime complaints lodged in Karachi relate to harassment over Facebook, according to data available with The Express Tribune.⁶

DOXXED AND THREATENED
Journalist Saba Eitzaz was forced to flee Pakistan after becoming the target of an online campaign that resulted in repeated online threats and sexual harassment, hacks, doxxing and character assassination. The campaign followed after her reporting on several high-profile stories of human rights abuses.⁷

POLICE OFFICER’S ARREST
The Supreme Court ordered the arrest of Deputy Inspector General of Gilgit-Baltistan, Junaid Arshad for harassing his former wife online. The police official blackmailed his victim by uploading objectionable photos on social media.⁸

PAKISTAN’S #METOO
- Pakistani actress Nadia Jamil shares her story of childhood abuse on Twitter. She is followed by entrepreneur Frieha Altaf, fashion designer Maheen Khan and thousands of others.
- Online music portal Patari’s co-founder Khalid Bajwa steps down after two women accuse him of sexual harassment through their social accounts.
- Pop star and model Meesha Shafi alleges singer/actor Ali Zafar sexually harassed her on more than one occasion. In response, Zafar files a defamation suit against her.
- Model Mujahid Rasool speaks out about personal experiences of sexual harassment, and the exploitation of male talent in the fashion industry.
- Over 50 women at Bahria College Islamabad accuse their college finals examiner Saadat Bashir of sexual harassment. The accusations came after student Saba Ali shared her story on social media. He is found guilty and fired.
- Philanthropist Faisal Edhi is accused of harassment by journalist Urooj Zia. Edhi denies the claim.
- Comedian and activist Junaid Akram is called out across social media for sexually harassing females. Akram denies the claim.

MISCELLANEOUS

CYBERCRIME

GANG BUSTED
Four members of a gang were arrested for running a racket that would ensnare Pakistani men settled abroad as well as rich men from other countries. The victims would be identified and tricked into marrying the female members of the gang through social media interactions. After marriage, the men would be drugged and compromising photos and videos would be taken to extort money from them. If the victims did not pay up, their photos/videos would be uploaded to social media. ⁹

CYBERCRIME CASE IN SINDH
A woman was arrested for blackmailing and harassing a man in Sindh. The harassment took place on Facebook and WhatsApp. The woman blackmailed the victim using objectionable pictures, extorting money from him. ¹⁰

DIGITAL CURRENCIES SCAM
Two men, Ahmed Butt and Malik Irfan were arrested for running an illegal digital currency business. The scam was being run under the names of First Coin, One Coin, Eagle Bit and Euro Coin. The accused looted millions of rupees from citizens who were tricked into investing in the company. ¹¹

ATM-HACKING
A member of an ATM-hacking gang, Amir Ghafoor, was arrested from Islamabad for hacking into ATMs across the capital. ATM-hacking came under the spotlight in December 2017 when it emerged that almost 600 bank customers had their money stolen by ATM hackers in Karachi. ¹²

DEFAMING THE ARMY
A First Information Report (FIR) was lodged against a man for insulting and abusing the Pakistan Army on Facebook. The FIR was lodged under Section 124-A of the Pakistan Penal Code (PPC) and Section 29-D of the Telegraph Act against Abdul Qayyum Arayin for posting messages and photos on his account against the Pakistan Army and Chief of Army Staff General Qamar Javed Bajwa. ¹³

---


A worrying trend seen across 2018 was massive leaks of data due to hacks and exploits in the banking sector, government institutions and popular mobile apps. These leaks, compounded with reported online monitoring of citizens by the state, lend credence to a United Nations report that expressed concern over increasing risks to privacy in Pakistan, emanating from state surveillance and a lack of digital security. The report stated that many governments, including Pakistan, Russia, China, Iran and Turkey, were neglecting or ignoring their duty to protect online encryption that helped ensure freedom of expression and privacy. At the same time, it noted that governments had adopted laws or proposed legislation that increased their surveillance powers, often in ways that fell short of human rights standards.¹

**MAJOR DATA BREACHES**

**CAREEM HACKED**

In April, popular ride hailing app Careem confirmed that the personal data of users and captains had been compromised in a giant breach. All users who had signed up with the service before January 2018 were affected.

> The hacked [Careem] data could be misused in several ways, and further threatens the safety of Careem users, because it includes critical information on the movement patterns of its users, including home and work addresses and other regularly visited locations.”

**USAMA KHILJI,**

Director of Bolo Bhi

---

Customer names, email addresses, phone numbers and most worryingly, trip history data (pick-up and drop-off points) had been stolen. Careem claimed that passwords and credit card information was not stolen.

At the time of the breach, there were 14 million customers and over 500,000 captains active on Careem across 13 countries. The company said it did not know the identity of the hacker(s).²

---

### DATA FOR SALE

Possibly the most alarming development of the year involved the leak of data of thousands of Pakistanis online through the Punjab Information Technology Board (PITB) and their access to NADRA records through API keys. According to one report, the leaks followed after NADRA gave access to its servers to PITB, which wanted to digitize citizens’ data and link it with departments such as education, health, police and land registry.³

The leak was uncovered over time as the data went on sale on Facebook/WhatsApp and Twitter, as well as through mobile apps. The sales included data of federal and provincial authorities; CNICs and personal data associated with them including family trees and criminal records; mobile numbers and names/addresses linked to them, plus call details; drivers license and locations. An investigation by Daily Times led to an anonymous ‘ethical hacker’ claiming to have hacked PITB. Another tech expert claimed that while PITB was not hacked, it was unauthorized access that could have led to the leak of data. Both PITB and NADRA distanced themselves from the issue and rejected the claims.⁴

At a later stage, then Chairman of PITB Dr. Umar Saif, alleged that PITB was actively revoking access of people who misused their access and said that departmental inquiries and action has been taken against the responsible personnel. He claimed all instances had been resolved.⁵

---


BANK ISLAMI HACKED, ALL BANKS HACKED?

The finance sector suffered a blow this year, when it was uncovered that BankIslami Pakistan was the victim of an overseas cyberattack that led to Rs2.6 million being stolen. This was the second big breach in the banking sector, with Habib Bank Limited customers having been attacked through ATM hacking using skimming devices at the end of 2017.⁶

The State Bank had immediately advised banks to ramp up security measures, especially regarding overseas transactions.⁷ But sometime after this high-profile case, the Director of FIA Cyber-Crimes wing Captain (retd) Mohammad Shoaib told the media that, “Almost all [Pakistani] banks’ data has been breached. According to the reports that we have, most of the banks have been affected.” The cybercrime chief’s alarming allegation followed after a report from cyber security firm Group-IB had stated that hackers had released a dump of Pakistani credit and debit cards on the dark web. “More than 100 cases [of cyber-attack] have been registered with the FIA and are under investigation. We have made several arrests in the case, including that of an international gang [last month],” Capt (retd) Shoaib had said.⁸

This claim resulted in an outcry, following which the State Bank released its own statement, categorically denying any hacks other than Bank Islami.⁹ The incident did lead to meetings between the FIA and SBP regarding online threats, in which the FIA shared details of 1,576 complaints received about banking fraud. However, SBP maintained that while threats exist, the banking sector was safe.¹⁰

VOTER DATA EXPOSED

The election year saw a major controversy in the form of a reported leak of voter data from the computerised electoral rolls system (CERS). The data was prepared and maintained by the National Database and Regulatory Authority (NADRA) under a contract with the Election Commission of Pakistan (ECP).

Allegations of a leak were first raised by PTI Chairman Imran Khan, who claimed that the database was leaked to PML-N – the party’s political rival. This was followed by a letter from the ECP to Nadra demanding an inquiry into the data leak. The letter also pointed out that Nadra had violated its agreement to protect the data. The data reportedly contained the age and religion of voters, which the PTI claimed would give the PML-N an unfair advantage in the run-up to the polls.¹²

A potentially greater privacy violation of millions of citizens came in the form of the government authorizing the ECP to provide voter data – including photos – in hard or soft form to candidates contesting the election, if they requested it. As highlighted in the media, this breach of privacy was made official through the Elections Act 2017 which stated that, “On the application of a candidate or his election agent, the district election commissioner or any officer authorised in this behalf by the commission shall provide to a candidate or an election agent a hard and searchable soft copy on universal serial bus (USB) in a portable document format (PDF) or any other tamper-proof format of the final electoral roll with photographs of the voters, and shall ensure that the copy is the same as provided to the returning officer and presiding officers”. A former ECP additional secretary had termed this sharing of private data “deceitful”.¹³

---


ACTIVISTS UNDER THREAT

A report by Amnesty International – Human Rights Under Surveillance: Digital Threats against Human Rights Defenders in Pakistan – outlined a dangerous trend that has become increasingly common over the last few years i.e. the surveillance, hacking and harassment of human rights activists.

The months long investigation uncovered digital attacks on activists including hacking of social media accounts, computers, mobile phones and social engineering ploys. Using digital forensics, Amnesty International was able to trace the attacks to individuals and companies based in Pakistan one of whom was a British-Pakistani cyber security expert, and another who used to work for the military’s PR wing.

While no evidence emerged of the state’s involvement, those targeted shared that they believed local intelligence agencies were behind the attacks.14

Amnesty International also noted that the online attacks appeared to be part of a larger effort to target civil society, including journalists, bloggers, protestors, activists etc. through means including intimidation, violence and enforced disappearances.

“As we uncovered an elaborate network of attackers who are using sophisticated and sinister methods to target human rights activists. Attacker use cleverly designed fake profiles to lure activists and then attack their electronic devices with spyware, exposing them to surveillance and fraud and even compromising their physical safety.”

SHERIF ELSAYED-ALI,
Director of Global Issues at Amnesty International

As stated at the release of the investigation, “As an elected member of the UN Human Rights Council, Pakistan has a responsibility to uphold the highest international standards. It has repeatedly vowed to protect human rights activists and criminalise enforced disappearances, but what we are seeing shows they have done nothing on this front while the situation is getting worse. The Pakistani authorities must immediately order an independent and effective investigation into these attacks and ensure that human rights defenders are protected both online and off.”15

DID YOU KNOW?

PTA devised new rules whereby data of every user logging into a public Wi-Fi Hotspot will be recorded and accessed when needed. Data recorded includes:

- Full name of the user
- CNIC number / passport numbers (in case of foreigners)
- Mobile number
- Acceptance of Terms and Conditions to use of such Data Services facilities
- Generation of the password through SMS
- Date and time of login/log off
- IP address allocated to the user
- MAC Address
- Internet Access Log (e.g. HTTP, POP, IMAP and more)16


CENSORSHIP AND MEDIA

Comment

Freedom Eroded

Sadaf Khan, Director Programs and Co-founder at Media Matters

Compared to traditional mediums, journalists still enjoy a little more freedom in the online space. We see comments and analysis on issues that never make it to mainstream media. We see more critical discussions. Journalists call out state censorship practices; something that is not possible outside the web.

This does not mean that there is no censorship online. There might be fewer legal instruments to control online speech, but there are still various means of intimidation that lead to self-censorship among journalists. A research conducted by Media Matters in 2018 found that journalists are self-censoring online in both professional and personal communications, which is demonstrative of the fact that the overall environment where free speech is restricted is creating pressure that extends to both online and offline spaces.

Offline, in mainstream media, red lines are clearly defined. They might not be written down, but they are well communicated and news outlets become a part of the censorship regime. Editors/management come under pressure from owners to stay away from sensitive topics. Online however, journalists do have a space of their own. So the decision to censor or not is largely their own. This is not to say that there are no external elements that influence their decision, but in the end it is the journalist who decides what kinds of risks they want to take. As a consequence though, if they do end up in trouble, they are less likely to garner support from the industry.
Hate speech is one way in which freedom of speech is being eroded online. One example would be the backlash against journalist and news anchor Asma Shirazi after her interview with former prime minister Nawaz Sharif was aired. As soon as it was made available online, Asma was targeted with hate speech and incitement to violence across social media. While hate speech is not a traditional way of imposing censorship, it does have a silencing effect on the targets.

Another way is harassment through official channels. We have heard cases of journalists getting letters from the FIA, and in some instances of devices being confiscated. More recently, there has been a flurry of notifications issued to journalists by Twitter, notifying them that their accounts have been ‘officially’ reported for illegal activity.

Tactics such as these are being used to impose censorship in the digital space, and this trend is likely to increase. The proposed Pakistan Media Regulatory Authority (PMRA) intends to introduce a similar regime of regulation online. In addition, we will see a growth in the ‘mob justice’ mentality online leading to a lot of hate speech, and consequent self-censorship.

**Freedom of speech was profoundly impacted this year in what appeared to be a well-coordinated, long-term effort.**

The major topics that were censored online and offline included:

- Coverage, sympathy and support for former prime minister Nawaz Sharif and his party the PML-N, who became embroiled in an expansive tussle with the military and judiciary.

- Support for the Pashtun Tahafuz Movement (PTM), a protest movement by young Pashtuns demanding answers from the state in connection to enforced disappearances, extrajudicial killings and mistreatment of the people of KP and FATA.

- Discussion of the ongoing insurgency in Balochistan led by groups of Baloch separatists who aim to break the province from Pakistan.

- Regional narratives that are seen as ‘anti-Pakistan’ such as criticism of friendly states China and Saudi Arabia, or support of India/betterment of Pak-India ties.

- Coverage and support for any extremist narratives and activities/protests on-ground or online.

- General criticism of the military and judiciary related to alleged interference in politics and erosion of democracy, especially specific to the general elections held in July.
A sustained effort was made to curb speech this year, with particular focus on media, and journalists who turned to the online space to share views they could no longer voice on traditional mediums.

As noted by media rights watchdog, Freedom Network (FN), more than 157 attacks on journalists took place between May 2017 and April 2018 of which 55 occurred in Islamabad. Senior editors and journalists termed this as one of the worst periods for press freedom in Pakistan. “[There] is pressure from the right, left and centre. I cannot write according to my own will. How can I be responsible if I am told what to write?” a former secretary general of the Pakistan Federal Union of Journalists shared in a news report.¹

Any media organization that did not conform to the prevailing narrative faced serious repercussions. The country’s biggest TV news channel Geo – seen as anti-establishment and sympathetic to PML-N – was blocked in many parts of the country, causing huge losses in advertising revenue. The move was condemned by the Human Rights Commission of Pakistan (HRCP). The organization pointed out that the fact that the ban was not sanctioned by media regulatory body PEMRA or by the information ministry was a cause for serious concern. It also noted that several regular English-language columns written with a focus on the PTM were deleted from newspapers’ online editions.²

Further indication of pressure on traditional media came when none of the top television channels covered a 10-day long peaceful protest by the PTM.³

The daily Dawn newspaper had its circulation blocked in parts of the country for reporting perceived as ‘anti-military’ and ‘pro-PML-N’. Newspaper sellers and shopkeepers confirmed that military and intelligence officers had instructed them to stop selling the paper. The punishing pressure now applied to Dawn and other news outlets is more insidious than the outright censorship of times past, Dawn’s editor, Zaffar Abbas had stated.⁴

Given the pressure on Dawn and Geo, Waseem Abbasi, Correspondent for The News shared that, “Other outlets have no chance. So basically they’re also falling in line.” ⁵

Given little space in the tightly controlled traditional media, many journalists took to social media to criticise the country’s establishment and perceived rigging of the elections. Some of these journalists came under direct threat.

---

Twitter manipulated Journalist Gul Bukhari’s account to ensure updates did not reach her followers. In an email, the social media company told her that her account had been reported but did not share by whom. She was then allowed to change her settings. Twitter also temporarily blocked PTM leader and activist Manzoor Pashteen account, assumingly for his vocal criticism of the state.⁷

In another instance, Twitter suspended accounts of Baloch political parties and prominent political leaders. The accounts were focused on the breakaway of the province of Balochistan from Pakistan.⁸

The reason behind Twitter agreeing to such measures could be earlier threats by the state to shut the platform in Pakistan in its entirety for non-cooperation with the government, framed under the issue of blasphemy.⁹ (See section: Blasphemy)

The army denied it had any role in the abduction¹⁰, but the perception of a real threat was established. The Director General ISPR Major General Asif Ghafoor had shared that the military, "have the capability to monitor social media as to who is doing what" adding that since January this year, more than 10,000 troll accounts had been created to target Pakistan and specifically the army. He said authorities had been alerted to probe these accounts.¹¹

Another prominent case was that of Ahmad Waqass Goraya who fled to the Netherlands after he and four other bloggers were picked up. Goraya, who has more than 19,000 Twitter followers, claimed his parents were told to keep him quiet “at least until the elections.”¹² Local journalist Taha Siddiqui – vocal in criticizing the military online – also fled the country after an abduction attempt in February.¹³

Vienna-based International Press Institute termed the situation “unprecedented”, citing journalists being intimidated, abducted and threatened and media houses being forced into self-censorship. Hameed Haroon, CEO Dawn Media Group and president of the All Pakistan Newspapers Society, said the military seeks to "influence the election results, influence the national narrative and liquidate the press".¹⁴


Respondents were asked to rate 11 reasons for why they self-censored. Majority of respondents said yes to these six reasons.

Source: Digital Rights Monitor report

GOVERNMENT RESPONSE

The chilling effect on free speech grew when the government announced plans to establish the Pakistan Media Regulatory Authority (PMRA) to oversee print, electronic and for the first time, social media. Journalists saw this as a move to curb media freedom.15

The government also announced a plan to develop a national level firewall system to block access to online content or websites. A proposal request for the system was issued. The firewall plan includes real-time traffic analysis to recognize objectionable content, block it and identify IP addresses of users trying to access it16 (also see sections: Blasphemy, Child pornography).

The firewall plan comes atop an already established censorship system through the installation of internet filtering system Netsweeper. An investigation by Citizen Lab found Pakistan to be one of the countries to have set up Netsweeper to filter content at the national-level, along with Afghanistan, Bahrain, India, Kuwait, Qatar, Somalia, Sudan, UAE and Yemen. It was uncovered that a wide range of digital content protected by international legal frameworks was being blocked, with Pakistan focused on censoring political news, opinion, and criticism.17

With regards to Facebook, the government spoke to a visiting team to discuss more venues of cooperation on filtering and blocking content for Pakistani users. Pakistan Telecommunication Authority’s Director General (DG) Internet Web Nisar Ahmed confirmed that, “Everything which is unlawful in Pakistan should be filtered for their users in Pakistan”. He had said that Facebook was profiting off the 35 million local Facebook users and as such should follow laws of the country.18

Source:
DID YOU KNOW?

Web Evaluation Cell (WEC) which was established by the Ministry of Religious Affairs and Inter-faith Harmony has been assigned to scrutinise websites that contain objectionable material or promote sectarianism.

A total of 6,149 websites were blocked by the Pakistan Telecommunication Authority (PTA) last year on the recommendation of WEC.

PTA had informed the Supreme Court (SC) that approximately 0.4 million websites promoting obscene content have been blocked by the body.

It has evaluated as many as 46,200 websites out of which 15,481 were those identified through complaints of the public.

Additional Attorney General (AAG) submitted a report on behalf of PTA, saying that 9,846 proxies had been blocked.

Source: Pakistan today report

CONFIRMED

Secure messaging service Telegram was banned under the instructions of the Pakistan Telecommunication Authority.19

FACEBOOK CENSORSHIP CASE STUDY

A Facebook post by the Dawn Media Group’s official page was blocked for Pakistani users of the social platform. The post was a link to a story in which firebrand politician Javed Hashmi criticized the judiciary and military. Facebook shared that, “Due to legal restrictions in your country, we’ve limited access to your post on Facebook”. The company did not clarify what law the Dawn.com post had violated, nor did it specify where the request had originated from. 20 The post was restored shortly after Dawn published an article on the censorship, with Facebook apologising for the content being "incorrectly restricted."


It’s an open secret in Pakistan that political parties and other institutions looking to influence public perception maintain social media teams that generate and disseminate fake news across platforms. In talks with The Diplomat, it was confirmed that leading political parties had asked their teams to create fake profiles as part of their social media strategy in the run-up to the elections.¹

In the same report, social media managers from the Pakistan Muslim League-Nawaz (PML-N), Pakistan Tehrik-e-Insaf (PTI) and Pakistan People’s Party (PPP) confirmed that creation of fake Facebook and Twitter accounts to propagate ‘their narratives was ‘official policy’.

“Everyone’s running fake Facebook accounts and Twitter bots, so we’re just keeping pace with what others are doing,” a PML-N social media executive had told The Diplomat. “It was the PTI that started this trend. So we’re just countering propaganda with propaganda”.

Other reports confirmed that social media teams were activated with a focus on the elections well before on-ground electioneering was kicked off by the parties. A Pakistan Today report uncovered all major parties hired a mix of social media professionals as well as volunteers to reach the widest online audience possible.²


SPREADING HATE ON TWITTER

A Trends Monitor report noted that hate speech connected to the elections had taken over a large part of the online space, with a significant amount of content being published by bots.

Monitoring 37 trending local hashtags on Twitter from June 23-30, the report stated that, “Propaganda-driven human-bots often used to push or engineer political campaigns, are deployed to harass, heckle and intimidate political rivals and journalists,” adding that some messages also incited direct violence.³

(See section: Censorship & Media)

PARTY STRATEGIES

Not all campaigning involved fake news and dubious accounts. A Dawn analysis of content showed parties and independent candidates were, “sharing campaign updates, linking surveys that are in favour of the party, uploading a large selection of campaign photos and videos and providing real-time updates of campaign activities from the ground, and criticism — of opponents and performance of previous governments.”

The PPP e.g. established a database of over 2.5 million members and operated 190 WhatsApp groups, according to one report. The party claimed its strategy was, “focused on the party’s manifesto and communicating our [projects] to the people.” Smaller parties like the Pak Sarzameen Party (PSP) had also set up digital teams with 300 volunteers and operating 120 WhatsApp groups down to the district level. The PTI, a party that first recognized the importance of online campaigning, spread its focus beyond social media to mobile apps. “The ‘one click to Imran Khan’ app will allow voters to [directly] send a message to the leader about key issues in their area. Every day, the best five to six questions will be shortlisted and Imran Khan will call the selected users to address their concerns,” the party’s social media secretary shared with Dawn. The ‘Insafian app’ meanwhile would allow candidates access to their constituents via GPS. All parties also recognized the need to communicate in Urdu and other regional languages online.⁴

Most [political] traffic on Facebook is rural-originated while Twitter is urban-driven

SHAHEER AHMED
Social media marketing expert

---


FACEBOOK’S ROLE

Facebook, under pressure after the disastrous findings of Russian interference in the US elections, released a statement through CEO Mark Zuckerberg promising to protect the integrity of the elections on their platforms. The Lahore High Court issued notices to the Pakistan Telecommunication Authority (PTA) chairman and Election Commission of Pakistan (ECP) regarding this, based on a petition requesting the government to request Facebook to take action against fake accounts set up for the elections. “The interim federal government, ECP and PTA should also be directed to regulate social media to ensure the democratic process is not harmed in the upcoming general election,” the petitioner upheld.⁵

“...there must be an open media environment that allows Pakistanis to fully enjoy their constitutional right of access to information... Worrisome occurrences have prevented the free distribution of news...appear to be aimed at intimidating journalists into silence.”⁶

On its end, Facebook committed to increasing the number of people working on safety and security issues around the world to 20,000, employing dedicated teams working on all upcoming elections including Pakistan’s. The company reportedly worked in collaboration with the Election Commission of Pakistan to tackle fake news, pages and accounts.⁷ One specific example of this effort was the disabling of numerous accounts and pages of the religio-political party Milli Muslim League (MML), which was led by alleged Mumbai terror attack mastermind Hafiz Saeed’s organization Jamaat-ud-Dawa. The MML termed this move censorship on the part of Facebook. ⁸

All these efforts did not have a significant impact however. As noted at one point by the Senate’s Standing Committee on Interior, mudslinging against candidates was rampant online. Examples were shared of political figures having their faces tacked onto images of dogs and donkeys. The FIA in response stated, “As objectionable material is being uploaded from abroad so it becomes difficult to take action. We are trying our best to investigate the matter and take action against the elements concerned, but there is a lack of coordination between the FIA and the Pakistan Telecommunication Authority (PTA).” ⁹ While reports of the FIA’s efforts were scant, one specific case emerged of the arrest of a PML-N supporter for allegedly running a Facebook page Ro Imran Ro” to malign PTI spokesman Fawad Chaudhry. The FIA cybercrime wing had acted on a complaint by Chaudhry that identified a “malicious” campaign against him was being run on social media, affecting his political image but, due to its sectarian nature, was also endangering his life (See section: Fake News).¹⁰

---

DID YOU KNOW?

Voter privacy was put at risk when the Election Commission of Pakistan (ECP) was authorized to distribute voter data, including photographs, to all candidates contesting the elections. The information could be requested in hard or soft copy.
*(Read more in section: Data Protection and Privacy)*

---

ACCOUNTABILITY GOES VIRAL

One positive aspect of social media in the general elections was holding politicians and political parties responsible thanks in large part to videos/photos capturing evidence of wrongdoing that would go viral across online platforms and then spread to mainstream TV.

The Asia Foundation noted in a report that many young people are increasingly engaged in the democratic process, particularly through the widespread use of social media. Sarwar Bari, an analyst at the Free and Fair Election Network (FAFEN), a democratic watchdog predicted that the election turnout would be “massive” if even half of the young voters who have seen and shared such videos go to the polls “it will strengthen the trust of the people in the democratic system.” In a similar vein, Shahzad Ahmed, director of Bytes for All, a digital rights group felt, “Social media has emerged as a democracy strengthening tool.”

---

LEAKED DATA

PTI chairman Imran Khan had accused the National Database and Regulatory Authority (NADRA) of leaking data to the PML-N to give the party an edge in the elections.
*(Read more in section: Data Protection and Privacy)*

Under-35s represented a massive proportion of the total electorate of 106 million voters registered in the 2018 elections. More than 17 million were in the 18-25 age bracket.

---

INTERNET VOTING

The elections in July saw online voting for the first time in the country’s history. The demand for online voting had been led by the Pakistan Tehreek-e-Insaf which enjoyed popular support among expats.

Following the Supreme Court’s approval, the National Database and Registration Authority (NADRA) was tasked with building out the database and platform to enable over seven million overseas Pakistanis to register and vote. Dubbed the ‘Internet Voting System for Overseas Pakistanis’, the project was to be developed at a cost of Rs150 million.12

The project faced criticism however, as a taskforce set up by the Election Commission of Pakistan (ECP) recommended against implementing e-voting following a technical audit of the platform. In a report, The Internet Voting Task Force (IVTF) said the iVote platform posed risks regarding transparent voting, which is a violation of Clause 94 of the Elections Act 2017 and Article 226 of the Constitution. Following tests and analyses, it added that the system "typically enables vote buying and voter coercion" and is also open to cyberattacks aimed at manipulating votes. 13

Two major political parties – the Pakistan People’s Party (PPP) and Pakistan Muslim League-Nawaz (PML-N) – both expressed concerns that online voting would be used to rig the elections. 14

The platform - www.overseasvoting.gov.pk - was eventually launched after the elections in late-August, in time for by-elections to be held in 37 constituencies in October.15

The registration period that lasted till mid-September proved to be an eye-opener however. Of the over 7 million overseas Pakistanis, only 632,000 were eligible to avail the facility, and of that number, only 7,419 completed registration.16

In total only 9,965 expats ever accessed the Overseas System.17
An ECP official later revealed that each of the final 6,233 votes cast by overseas Pakistanis cost the national exchequer over Rs15,000. A total of Rs95 million was spent on the project. 18

“"The i-voting system being put into place is flawed from its inception and has the ingredients of becoming a tool in the hands of forces that may want to manipulate elections in Pakistan.”

FORMER SENATE CHAIRMAN RAZA RABBANI

REGISTERED OVERSEAS VOTERS

<table>
<thead>
<tr>
<th>Constituency</th>
<th>Reg. Voters</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA-243 (Karachi East 2)</td>
<td>1353</td>
</tr>
<tr>
<td>NA-131 (Lahore IX)</td>
<td>1126</td>
</tr>
<tr>
<td>NA-69 (Gujrat II)</td>
<td>698</td>
</tr>
<tr>
<td>NA-53 (Islamabad II)</td>
<td>641</td>
</tr>
<tr>
<td>NA-60 (Rawalpindi IV)</td>
<td>567</td>
</tr>
<tr>
<td>NA-124 (Lahore II)</td>
<td>510</td>
</tr>
<tr>
<td>NA-63 (Rawalpindi XII)</td>
<td>321</td>
</tr>
<tr>
<td>NA-65 (Chakwal-II)</td>
<td>312</td>
</tr>
<tr>
<td>NA-35 (Bannu)</td>
<td>304</td>
</tr>
<tr>
<td>NA-56 (Attock-II)</td>
<td>230</td>
</tr>
<tr>
<td>NA-103 (Faisalabad-III)</td>
<td>68</td>
</tr>
</tbody>
</table>

The fake news phenomenon in Pakistan grew steadily across 2019, with misinformation spreading through social media, and particularly, Facebook and WhatsApp.

A number of these fake stories, which targeted institutions such as the military and judiciary, were also amplified by mainstream media, including TV news channels, further exacerbating the problem.

In some cases, it was clear that the news had been manufactured with the intent to deceive, while some appeared to be cases of misunderstanding and poor reporting/fact checking on the part of the media and/or ordinary citizens.

Attempting to address the problem, the Ministry of Information and Broadcasting launched an official Twitter account @FakeNews_Buster to highlight misinformation.¹ This effort was criticized however and alleged to be an attempt by the government to defend itself by framing real news as fake, and to target opponents.

A list of some prominent cases that emerged follows, however, this does not capture the extent of the issue as a vast majority of fake news is not identified and refuted. In cases where it is debunked, in general the correction/explanation does not achieve the same level of virality as the original misinformation.

**WRONG PHOTO, WRONG THIEF**

A Pakistani civil servant, Zarar Haider Khan, was placed under investigation for stealing the wallet of a visiting Kuwaiti delegate at a function. CCTV footage of the robbery was shown on TV channels and shared online. Shortly after, a photograph of the suspect was also shared widely.

However, the photograph turned out to be that of an innocent man residing in the United States whose name, Ziad Haider, was somewhat similar to the suspect, and assumedly the reason why it got shared. While it was widely reported that the photograph was incorrect, many videos and reports containing the photo with the original mistake remained online.²

---

**BEACONHOUSE HATE CAMPAIGN**

A hashtag #BoycottBeaconHouse trended on Twitter for some time, labeling the school as an ‘enemy of the state’. Misinformation was critical in making the campaign viral; the school system was accused of using books showing the wrong map of Pakistan, in which Kashmir was identified as a part of India. In reality, the issue had been identified as far back as 2015 and was since then being corrected in all text books that were printed by The Educators and provided to the school. The mistake was also never replicated in any text books printed by Beaconhouse itself.

Additionally, incorrect news was shared that Beaconhouse was exclusively using a problematic Oxford University Press Pak Studies textbook, when in fact many schools were using the book. Finally, the campaign falsely attributed a past Pak Studies exam paper with similar issues to be exclusive to Beaconhouse, whereas the paper was actually a Cambridge O Level exam.³

The Beaconhouse administration claimed that the "engineered hate campaign" was launched by an ex-employee of The Educators — a school system running parallel to Beaconhouse.⁴

---


DURAND LINE ‘ACCEPTED’

A fake Facebook post screenshot disguised as content from Dawn.com was shared widely online, claiming that Afghan National Security Adviser Hanif Atmar and Chief of Army Staff Gen Qamar Javed Bajwa held a meeting in which Afghanistan accepted the Durand Line as an official border.

This extremely sensitive regional matter, seemingly coming from a large, reputed news organization prompted the Afghan National Security Council (NSC) to issue a statement clarifying no such agreement was reached. Dawn later clarified that the screenshot was fake, and identified visual/editorial mistakes made in the image.⁵


‘RO IMRAN RO’

The admin of a Facebook page, ‘Ro Imran Ro’ was arrested for disseminating misinformation, and specifically about Pakistan Tehreek-i-Insaf (PTI) spokesman Fawad Chaudhry.

Updates on the page that linked Chaudhry to Mumtaz Qadri, the man who had assassinated Punjab Governor Salmaan Taseer led to a complaint by the spokesperson to the FIA cybercrime wing, who carried out the arrest. It was alleged that the fake posts were not only damaging to Chaudhry’s political career, but also stirring sectarian hatred that could endanger his life.⁶

EMERGENCY LANDING

A video was widely shared on social media showing a PIA plane on fire, with claims that an emergency landing had taken place. PIA later clarified that this was fake news: “No emergency landing has taken place anywhere. The animated video of an old PIA plane (not in use) caught with fire circulating in media is fake. We strongly condemn this malicious and criminal act to defame [the PIA].”⁷

SECURITY ALERTS

Dozens of fake security alerts were shared across social media and particularly through WhatsApp this year, continuing a trend that emerged in 2017. The posts gained considerable mileage due to the serious nature of the content and the use of names of reputed security agencies, including the military.

The situation reached a point where the military’s media wing, Inter-Services Public Relations (ISPR), had to send out updates warning citizens that fake threat alerts were being spread using the military’s name. The ISPR termed these alerts ‘propaganda’ suggesting an organized attempt to mislead the public.⁸


Rumors that former prime minister Nawaz Sharif’s daughter Maryam Nawaz was pregnant made the rounds on social media based off a doctored screenshot presented to be an article on Dawn.com. To give the fake story weight, it was written that the news organisation had obtained her medical reports that proved Maryam was expecting.

Dawn later published an article debunking the news and pointing out mistakes made in the screenshot that proved it was fake.⁹

In October, Avi Schraf an Editor of Israeli daily Haaretz tweeted that a private plane had travelled from Israel to Pakistan, landed for 10 hours, and then flew back. The editor backed up his claim with screenshots from a real-time air traffic website.¹⁰

What followed was a wave of speculation, intrigue and outrage across social media, followed quickly by amplification on traditional media in Pakistan. The rumor that took form was that Israeli PM Benjamin Netanyahu flew to the country to hold secret talks, with some narratives suggesting this was the start of new relations with Israel. It was even suggested this meeting was part of a broader reimagining of ties with India as well.

The government was quick to term this development as ‘fake news’ and the various narratives surrounding it as propaganda.¹¹

---


CRACKDOWN ON SOCIAL MEDIA

A ‘breaking news’ screenshot of a DawnNews TV report was circulated on social media suggesting that the newly elected government was going to kick off a crackdown on social media accounts targeting the state – a move assumedly aimed to quash criticism and free speech.

In a response, the screenshot – widely shared by supporters of political parties forming the opposition – was identified by Dawn as authentic, but entirely misleading as it was aired a year ago in March 2017, and was actually a move that had been announced by the previous government to protect itself from criticism.12

PAKISTANI STUDENT BEATEN IN CHINA

A video of a young man being assaulted in China went viral locally, as it was framed as the beating of a Pakistani student, Usama Ahmad Khan.

It was later clarified by a Foreign Office spokesperson that this was misinformation, as the Pakistani student in question had committed suicide in Shenyang city in China’s Liaoning province, and was not the young man in the video.13

HIGH-PROFILE DAM FUND DONORS

Following the announcement of the establishment of a crowd-funded ‘dam fund’ for construction of the Diamer-Basha Dam, a string of fake announcements of support/contributions by high-profile personalities were circulated online.14

At various points, donations worth millions of dollars were falsely attributed to:

- Pakistani-American billionaire Shahid Khan
- Facebook chief Mark Zuckerberg
- Former president Pervez Musharraf

---


CHIEF JUSTICE’S EXPENSIVE TASTES

Multiple social media campaigns were launched during then Chief Justice of Pakistan (CJP) Saqib Nisar’s visit to the UK to raise funds for the construction of dams. The campaigns claimed that the chief justice was staying at one of London’s most expensive hotels – the Dorchester Hotel. Media reports later debunked this claim, as it turned out the CJP and his family were staying at the Marriott Hotel, and the cost of the rooms was borne by Nisar himself.¹⁵

AASIA HAS LEFT PAKISTAN

While it is unclear whether the rumor originated online or on TV channels, reports that Aasia Bibi, a Christian woman acquitted of blasphemy charges, and resultant narratives of how she was flown out of the country and where she travelled to became an online, viral phenomenon.

The Supreme Court’s decision to drop charges against Aasia had resulted in days of violent protests across the country, and this rumor was arguably part of fueling a dangerous, on-ground situation.

The government denied the report and dubbed it fake news. In truth, Aasia had been flown from a Multan jail to Islamabad.¹⁶


It has become a norm to publish fake news for sake of headlines, #AsiaBibi case is sensitive issue it was extremely irresponsible to publish news of her leaving the country without confirmation, I strongly urge section of media to act responsible

Ch Fawad Hussain ☑️
@fawadchaudhry

It has become a norm to publish fake news for sake of headlines, #AsiaBibi case is sensitive issue it was extremely irresponsible to publish news of her leaving the country without confirmation, I strongly urge section of media to act responsible

❤️ 11.8K  10:29 AM - Nov 8, 2018
MISINFORMATION TRACKED

AFP Fact Check is a project aimed at 'fact-checking in response to the multiplication of misinformation and disinformation online'. Below is a list of Pakistan-related fake news they debunked in 2018.

- An entire cricket team was bowled out for zero (Facebook post)
- Mufti Abdul Qavi appointed as an advisor for religious affairs by Imran Khan (Online article)
- 50,000 PML-N supporters rallied in Lahore on Nawaz Sharif’s return and arrest (Photos/videos)
- Imran Khan’s ex-wife Reham kissed an American on a US TV show (Online article/video)
- Polling officer allowed cheating during the elections (Video)
- Cricket match between Sri Lanka and South Africa (Facebook post)
- Edward Snowden says Osama bin Laden is living in the Bahamas (Online article)
- Punjab University student caught having sex in Jinnah Garden (Video)
- Documents show CIA assassinated prime minister Liaquat Ali Khan (Online article)
- MTV presenter Kristiane Backer converted to Islam by Imran Khan (Online article)
- Orange Line becomes most expensive mega-transit project globally (Online article)
- Trident chewing gum contains pork, is haram (Newspaper article)
- Schoolboy is kidnapped in Karachi (Video)
- Government announced no govt employee would be sacked (Online article)
- Pakistan's new high-tech automatic anti-tank system (Video)
- Pakistan to have flying cars through Uber (Online article)
- PTI legislator appointed head of nationwide welfare programme (Social media posts)
- Pakistan ranking on TI Corruption Perception Index improves from 175 to 116 (Facebook post)
- Israeli PM Benjamin Netanyahu meets Imran Khan (Social media posts)
- Asia Bibi meets Pope Francis after being acquitted in blasphemy case (Video)
- PM Imran Khan said Jesus Christ never existed (Online articles)
- Michael Jackson sings “Give thanks to Allah” (Video)
- Government cuts petrol prices to Rs20/litre (Facebook post)
The way forward

Ali Sarfraz, CEO Karandaaz

There has been an upswing on the fin-tech front, with an emphasis on providing services, but the focus has been on payments and lending with little attention or effort going towards savings, insurance and investment. These areas are still very weak. Companies are also spending a lot more on developing customer identification and credit scoring models.

The function of the market is such that companies in Pakistan are trying to provide end-to-end services. This is because the market is very small, but that means companies want to become monopolies (Telenor and Jazz wallets is an example).

There is an opportunity for partnership between companies, especially in terms of credit, but that opportunity is not being availed fully. Take a look at PSO
and PSP licenses; apart from these two channels, what kind of scale are companies offering?

Financial inclusion in Pakistan is only at 21%. There needs to be more work done here. Also, Google Pay may be looking to enter the market, but what’s missing is the underlying infrastructure, as OneLink is not enough. PayPal specifically could help freelancers locally and would also improve fintech in the country. The government is keen on capturing remittances, but problems with regulators might bar PayPal’s entry for now.

This is the right time to enter the market however; access to the internet and access to smartphones is increasing.

**WHAT NEEDS TO BE DONE**

Currently, there are three classes of layers in the industry:

1. Mass wallet issuers, which includes Telenor
2. Niche wallet issuers, which includes UBL Omni
3. Fin-tech, with companies like Finja and Inov8

The key to moving ahead in this arena is implementing a regulatory sandbox i.e. mechanisms for developing regulation that keeps up with the fast pace of innovation.

- Fin-tech is wary of banks. Services are limited and handicapped; they should be within risk management.
- Democratization of customer data is important. Entities rely too heavily on consent architecture.
- There should be a low cost payment system. Currently, if a customer wants to transfer Rs10, the charges amount to a much higher cost than what was originally sent/transferred.
- There is no Directory Function. Transfers should be made possible based on your CNIC numbers.
- The government should push payments electronically.
- The industry should incentivize individuals, businesses, innovator and consumers. By lowering taxes, a market is created which puts money back in the system. In Pakistan people save in hard cash. This needs to change to bring savings into the fold.

**3 MAJOR OPPORTUNITIES**

1. Using mobile phone cameras for customer identification. Fingerprints or photos taken from ordinary smartphones can be connected to the NADRA database.
2. QR code—phone pay. That’s the future. A QR code reader can be downloaded onto a smartphone by anyone, and they are mostly free of charge. This means that any customer can walk into your business with his or her smartphone, and scan a QR code which you have generated.
3. Use of over-the-counter for e-commerce. PSO/PSP channels connect consumer centers with production centers due to good logistics and a robust payment system.
Fin-tech and the banking sector’s expansion online saw a number of major developments across the year.

**BIG ENTRANTS, KEY PLAYERS**

The announcement of the upcoming arrival of three financial technology (fin-tech) companies - FonePay, Monet and TPL Rupya - to Pakistan was seen as an indicator of healthy growth in the finance sector. The companies’ offerings would allow online transactions to be made to anyone on any mobile wallet account.¹

According to a February report, Fonepay had already connected with 50,000 shops for QR code payments and expected to grow five times by end of 2018. “The fintech expects to engage 250,000 shops across the country by the end of 2018,” Muhammad Ziaul Haq, Head of Acceptance Inov8 Limited – the parent company of Fonepay – had shared.²

In August, it was shared that Alipay, the China-based third party mobile and online payments platform would start operating in Pakistan. This was shared by Telenor chief executive officer Irfan Wahab Khan, a board member of the Telenor Microfinance Bank in which Ant Financial, the parent company of Alipay and the financial services affiliate of Alibaba, acquired a 45% stake at an investment of $184.5 million in March.³ Telenor is one of the major telcos in Pakistan offering mobile-based branchless banking services (Telenor’s Easypaisa) alongside competitor Mobilink (Jazz Mobicash) and United Bank Limited’s Omni. ⁴

$36 billion

is the market potential of
digital financial services
in Pakistan by 2025

In August, it was shared that Alipay, the China-based third party mobile and online payments platform would start operating in Pakistan. This was shared by Telenor chief executive officer Irfan Wahab Khan, a board member of the Telenor Microfinance Bank in which Ant Financial, the parent company of Alipay and the financial services affiliate of Alibaba, acquired a 45% stake at an investment of $184.5 million in March.³ Telenor is one of the major telcos in Pakistan offering mobile-based branchless banking services (Telenor’s Easypaisa) alongside competitor Mobilink (Jazz Mobicash) and United Bank Limited’s Omni. ⁴

**QUATERLY HIGHLIGHTS**

- BB Accounts increased by 1.9% to reach 39.2 million and active BB accounts increased by 9.3% to reach 21.8 million.
- BB transactions grew by 12% and 18% in volume and value respectively.
- Rs. 37.9 billion disbursed on account of social welfare payments using BB channels.
- An average of 2.4 million transactions conducted per day during the quarter.

Source: SBP

**BB ACCOUNT GROWTH AND ACTIVITY**

(No. of Accounts in millions)

<table>
<thead>
<tr>
<th></th>
<th>Jun '17</th>
<th>Sept '17</th>
<th>Dec '17</th>
<th>Mar '18</th>
<th>Jun '18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Accounts</td>
<td>27.3</td>
<td>33.1</td>
<td>37.3</td>
<td>38.5</td>
<td>39.2</td>
</tr>
<tr>
<td>Active Accounts</td>
<td>13.2</td>
<td>15.5</td>
<td>19.3</td>
<td>20.0</td>
<td>21.8</td>
</tr>
</tbody>
</table>

Source: SBP

---


Additionally, the telcos and some independent startups are all offering mobile wallets for easy financial transactions. According to data compiled by the industry, telcos are conducting monthly transactions worth billions of rupees through mobile wallet accounts. They have over 400,000 retailers across the country. This massive growth has however prompted concerns related to money laundering and terror-financing for the Financial Action Task Force (FATF) as well as the State Bank looking to regulate such products.

“Approximately 90 percent of e-commerce transactions in Pakistan are cash on delivery… From the consumer side, a preference for cash may be attributed to low financial and digital literacy, security of online payment channels and instruments, and availability of dispute resolution mechanism in case a wrong or substandard product is delivered to the customers.”

STATE BANK REPORT

Perhaps the biggest potential entrant discussed across the year has been US-based financial services giant PayPal, which allows for online money transfers. The company operates in 190 markets globally, but has not entered Pakistan.

Newly appointed Finance Minister Asad Umar gave the IT ministry four months to convince PayPal to come to Pakistan, going as far as to say that he would personally convince the PayPal CEO if needed. The ministry was asked to form a task force to this end, failing which they were to begin work to launch a home-grown online payment system.

PayPal’s entry to Pakistan could reportedly facilitate 200,000 freelancers, who earn more than $500 million but still use non-banking channels to receive payments. The e-commerce industry would be set to benefit from the move as well.

“During 2016-17, Pakistan’s IT exports were $3.3 billion, which have jumped to $5 billion and are expected to grow to $6 billion next year”

SAIF AKHTAR
Co-Founder of technology start-up accelerator and seed fund 10XC

---


According to a McKinsey & Company report, fin-tech in Pakistan will result in:

- **4 million** new jobs
- **93 million** bank accounts
- **$36 billion** added annually to gross national product (GNP)
- **$7 billion** to Pakistan government’s net revenue by 2025

It outlines that the impact of digital financial services may come through increased bank lending to SMEs and households and a shift in savings to digital accounts. This would encourage growth in self-employment and more startups.⁷

*CRYPTOCURRENCIES BANNED*

The cryptocurrency market surge – led by Bitcoin – at the end of 2017 caused a stir in Pakistan as well, resulting in a largely informal exchange of digital currencies between individuals through bank transfers and even cash payments. It also prompted the establishment of Urdubit.com, the ‘first and only Bitcoin exchange in Pakistan’ that saw regular trading up until April, when the State Bank issued a notice banning all investment and trading in cryptocurrencies.

“All banks, development financial institutions, microfinance banks and payment system operators, payment service providers are advised to refrain from processing, using, trading, holding, transferring value, promoting and investing in virtual currencies/tokens. Further, they will not facilitate their customers/account holders to transact in VCs/ICO Tokens. Any transaction in this regard shall immediately be reported to the Financial Monitoring Unit (FMU) as a suspicious transaction,” the SBP stated.⁹

Major reasons cited for the ban was the dangers of scams and security concerns raised by the inability to track what the money was being used for.¹⁰

---


E-COMMERCE

STATE BANK OF PAKISTAN STATS

Rs99.3 billion
Is the size of Pakistan’s e-commerce market in FY18.

92%
Is the market year-on-year growth (FY17 was sized as Rs51.8 billion)

Rs 40.1 billion
Is the sales figure for local and international e-commerce merchants in FY18

8 banks
Are on-boarding e-commerce merchants

10
Branchless banking providers are operating in Pakistan

ESTIMATES OF ECOMMERCE IN PAKISTAN

*If we go by market estimates, the share of digital payments is about 40 percent in the total e-commerce transactions by value. For FY19 and FY20, a YoY increase of 25 percent in digital sales is expected.

Data source: SBP for actual digital transactions; market estimates for forecast

<table>
<thead>
<tr>
<th></th>
<th>FY16E</th>
<th>FY17</th>
<th>FY18</th>
<th>FY19F</th>
<th>FY20F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total* (Digital plus COD)</td>
<td></td>
<td></td>
<td>99.3</td>
<td>126.4</td>
<td>158.0</td>
</tr>
<tr>
<td>Domestic Digital</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Foreign Digital</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
35% of Pakistan’s monthly 70,000 Cash-on-delivery shipments are delivered outside of Karachi, Lahore, and Islamabad.

JAWAD FARID
Head of corporate innovation at Excellence Delivered (ExD)

**NUMBER OF E-COMMERCE MERCHANTS ACCEPTING DIGITAL PAYMENTS IN PAKISTAN**

Data Source: State Bank of Pakistan

<table>
<thead>
<tr>
<th></th>
<th>FY17</th>
<th>Q1-FY18</th>
<th>Q2-FY18</th>
<th>Q3-FY18</th>
<th>Q4-FY18</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>571</td>
<td>812</td>
<td>905</td>
<td>1,023</td>
<td>1,094</td>
</tr>
</tbody>
</table>

**PAYMENT MODE SELECTION BY VALUE**

Data Source: SBP, market estimates

- 55% TOTAL DIGITAL PAYMENTS
- 40% IBFT/Card swipe on delivery
- 22% COD

**UNCTAD B2C E-COMMERCE READINESS INDEX* 2017 RANKING (OUT OF 144 COUNTRIES)**

Data Source: UN Conference on Trade and Development

<table>
<thead>
<tr>
<th>Country</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>65</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>73</td>
</tr>
<tr>
<td>Vietnam</td>
<td>74</td>
</tr>
<tr>
<td>India</td>
<td>83</td>
</tr>
<tr>
<td>Philippines</td>
<td>96</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>103</td>
</tr>
<tr>
<td>Nepal</td>
<td>108</td>
</tr>
<tr>
<td>Pakistan</td>
<td>120</td>
</tr>
</tbody>
</table>

*Reflects processes involved in an online shopping B2C transaction. It is calculated by using data pertaining to number of internet users; number of secure servers; the Findex account penetration score; and the postal reliability (logistics) score.
STRUCTURE OF E-COMMERCE IN PAKISTAN AND MAJOR PLAYERS

E-Commerce in Pakistan

- Business to Customer (B2C)
  - Goods (one-to-many; Khaadi)
  - Services; (e.g. PIA online; Metrocab)

- Online marketplaces for goods (many to many)
  - Own inventory & delivery (e.g. ShopHive, Homeshopping)
  - 3rd party sellers (Daraz, Yayvo, Foodpanda)
  - Infomediaries
    - Property (Zameen.com); Jobs (rozee); General Classified (OLX)

- Online marketplaces for services (many to many)
  - Immediate delivery
    - Transport (Careem); bookme.pk

LOGISTICS FIRMS FOCUSING ON E-COMMERCE

Source: SBP

- PAKISTAN POST
- TCS
- OCS
- LEOPARD
- CHEETAY
THE CASH ON DELIVERY CHALLENGE

Pakistan is still struggling to resolve the issue of easy online payments, and that continues to negatively impact e-commerce. The State Bank of Pakistan has noted that a majority of payments are still being made using the cash-on-delivery (COD) model. The major challenges that need to be overcome include:

01 Get people into the banking system:
At the moment only 21% of the population has a bank account, making COD the only route to make payments for many. Under the 2018 Digital Pakistan policy, SBP is preparing to launch a national payment gateway to promote internet merchant accounts to facilitate transactions.¹ There are also efforts being made to improve branchless banking offerings, fintech solutions and getting big players like PayPal into the country (See section: Fintech and Banking).

02 Greater internet penetration:
While overall penetration has increased, access to high-speed internet is still low, and many areas still remain with poor or no connectivity (See section: Internet Access). Without meaningful internet access, e-commerce activities are limited or not possible.

03 Increase consumer awareness and protection:
The population is still unaware of e-commerce platforms/products/services, the process of making purchases, payment options and how they work, and there is additional lack of trust in making online payments. As the SBP noted: “A major issue that keeps consumers from adopting advance payment mechanisms is the fear that their products might not be delivered or they might be different in nature or quality from the items mentioned online... From the consumer perspective, a preference for cash and low financial literacy accentuates the need for COD. Even those customers who are financially literate feel hesitant to share their personal information online due to security concerns.”²

“An heavily taxed broadband internet limits penetration and growth of e-commerce and the digital economy, marring the potential for jobs and exports.”

EHSAN MALIK
CEO of Pakistan Business Council

E-COMMERCE POLICY FINALISED

The Ministry of Commerce (MoC) took a major step forward early in this year by finalizing the policy framework for e-commerce and digital trade. The exercise took two years and was executed by a National Advisory Council (NAC) on e-commerce and an E-commerce Policy Unit (ECPU) comprising public and private sector stakeholders.³ Parameters of the proposed policy that have been identified by the PMO are availability and reliability of the Information and Communications Technology (ICT) platforms, development of supportive financial services regulations, regulatory framework, establishment and regulation of e-commerce establishments, conducive import and export regulations, taxation issues, coordination, consultation, cooperation and oversight.

THE ACTION PLAN CONSISTS OF:

- Enactment of national laws on consumer protection which may include provisions for seller protection, specifying rights, obligations, liabilities and penalties for both sellers and consumers.

- Enactment of privacy and data protection laws including provisions for e-transaction to enable e-contracts.

- Amendments in the foreign exchange regulations of SBP to facilitate cross-border electronic transactions.

- Establishment of dispute resolution mechanisms for e-commerce.

- Formulation of licensing requirements for establishing and operating e-commerce businesses.

- Subsidising UST rates and other tax relaxations for e-commerce on products where sales are made on online portals in order to encourage selling online.

- Provision of safe and secure platforms for financial transactions online.

- Establish a working group on e-commerce.

- World Trade Organisation (WTO) to constantly liaise with Pakistan’s permanent mission to WTO in order to assist them for the upcoming multilateral discipline on e-commerce.

- Finalisation of the National Payment Gateway (NPG) for international transactions.

- Simplification of import and export procedures and requirements and border measures and logistics arrangements for the purpose of facilitating e-trade.

IMPROVING THE CONSUMER EXPERIENCE

The following are suggested steps that can reduce threats to e-commerce culture:

- Provide proper training to content writers and vendors to present their products correctly.
- Improve the in-store system of ‘Product Reviews.’
- Improve customer service as well as ‘After Sale Services.’
- Allow users to report a seller directly and easily to the concerned management.
- Take necessary action against incompetent vendors.
- Strict action needs to be taken against scamming sellers under cybercrime, and affected buyers should be compensated on a priority basis.
- Stay in constant communication with other stores, share information regarding guilty sellers and discourage others from walking the same path by making the information public.

Extract from ‘12 reasons Pakistanis avoid buying things online — and how that can change’ by Munir Rahool, tech writer for Dawn.com
ALIBABA ENTERS PAKISTAN

Multinational conglomerate Alibaba Group opted to enter Pakistan in 2018 with the complete acquisition of e-commerce site Daraz.pk – a move that is expected to have a major impact on the local industry. The deal was reportedly between $450-500 million. The world’s largest retailer and e-commerce company reportedly also had affiliate Antfinancial acquire 45.4% of Telenor Microfinance Bank i.e. Easy Paisa in a move to cement its position regarding e-payment options in the country.⁴

Badar Khushnood, VP of Growth at Fishry.com and Head of E-commerce Committee at P@SHA (Pakistan Software Houses Association) termed this development as an “excellent opportunity for Pakistan”.

“Most foreign direct investment has been in the telecom sector. This would be the next big emerging sector. Foreign investors have been hesitant and feared entering Pakistan. Now that a giant like Alibaba has entered Pakistan, there will be followers. Potential investors and companies which couldn’t bear the cost of due diligence will now follow Alibaba. So far Google, FaceBook and Twitter have been hesitant to enter Pakistan due to legal issue, law and order. So this is a good development,” he shared.

Regarding fears that local players will not be able to compete, Syed Salman Hassan, CEO TCS Ecom (which owns e-commerce site Yayvo.com) shared that the e-commerce market has vast potential for growth. “The potential of the Pakistani consumers – 200 million plus population with 65pc below the age of 30 – is finally being realised. With Alibaba entering in the local market, it will get better from here onwards. Jack Ma and Alibaba have been supportive of the small-and medium-enterprises sector and China is proof.”

Another fear expressed by Barkan Saeed, Chairman of Pakistan Software Houses Association, relates to existing government policies that hurt the business environment and discourage new entrants. “If Alibaba decides not to expand further in Pakistan due to our environment, that would be a big loss… We have to act quickly and decisively.” ⁵


Bytes for All (B4A), Pakistan is a human rights organization and a research think tank with a focus on Information and Communication Technologies (ICTs). It experiments with and organizes debate on the relevance of ICTs for sustainable development and strengthening human rights movements in the country. Its strategic plan delivers in following key result areas (KRA), which include:

1. Securing digital rights and freedom of expression for civil liberties;
2. Strengthening digital security of human rights defenders & media professionals;
3. Ending technology-driven gender-based violence;
4. Network building at national, regional and global level; and
5. Community development and communications for environmental sustainability

To deliver above-mentioned KRAs, B4A conducts research for evidence-based policy advocacy and capacity building of human rights defenders on their digital security, online safety & privacy.

Globally acclaimed Take Back The Tech Campaign is the flagship of Bytes for All, which focuses on strategic use of ICTs by women and girls to fight violence against women in Pakistan.
A REPORT BY BYTES FOR ALL, PAKISTAN
Author: 
**Jahanzaib Haque**
(jahanzaib.haque@gmail.com)

Research Assistant: 
**ShahBano Ali Khan**

Design: 
**Alyna Butt**
(alynaabutt@gmail.com)