



# Will China export its illiberal innovation?

Products created for China's vast surveilled and censored domestic market are increasingly popular overseas

## NICK FRISCH

The author is an Asian studies doctoral candidate at Yale's graduate school, and a resident fellow at Yale Law School's Information Society Project

**I**N 2009, AFTER internet-fuelled race riots between Uighur Muslims and Han Chinese in China's north-east territory of Xinjiang, the ruling Communist Party took drastic action: the digital kill switch. Beijing disabled Xinjiang's internet, sending military police to restore order. The blackout lasted nearly a year. Now, a decade later, Xinjiang is writhing under a new clampdown aimed at the Uighurs. This time, Beijing has embraced the opposite philosophy: a digital panopticon, or surveillance state. It aims to expand China's Internet of Things and enmesh its own people.

The technologies being honed in Xinjiang, driven by this kind of illiberal innovation, may be coming soon to an app store near you. These exports risk enabling aspiring autocrats worldwide, and may concentrate alarming power in the hands of China's Communist Party.

Until recently, China was dismissed as an innovation laggard that copied technology from the West. Today, many Chinese tech sectors have leapfrogged Silicon Valley, sometimes with heavy-handed help from the party. Consumer-friendly smartphone apps have pushed cash, credit cards and identification documents towards extinction. Hotel booking systems will ping your smartphone, linked to your national ID card, to let you check in using facial recognition. In under a minute, a mom-and-pop hardware kiosk can create a personalised QR code for cashless payments through WeChat, an indispensable app that combines the functions of WhatsApp, Venmo, Seamless, Uber and more. For an expatriate accustomed to China's free-wheeling start-up scene and whizzy tech conveniences, coming home can feel like stepping back in time.

But, as the Uighur minority of Xinjiang are learning, that convenience comes at an Orwellian price. Speedy data networks and integrated digital commerce are learning to work with the party's aggressive security apparatus. Invasive DNA databases and facial recognition powered by artificial intelligence have created a digital dragnet, enhanced by mandatory surveillance

apps installed on smartphones and backed by a newly built network of IRL gulags. Offences as trivial as forwarding a traditional Islamic holiday greeting on WeChat, or posting a bearded selfie, can land citizens in internment camps. Even Uighurs living abroad are entangled, through their families and their smartphones, in Beijing's crackdown. (The repression has reportedly created a black market in old Nokia phones, which are less legible to the state.)

Xinjiang's plight is more than a local tragedy: It is a warning.

The global risk from China's technology sector is not necessarily a sinister conspiracy to exert Xinjiang-style controls overseas. Beijing's leaders are focused on domestic affairs and for now, China's budding tech dystopia is still more "Brazil" than "Black Mirror." Rather, this risk is a byproduct of Beijing's business as usual, on a huge global scale.

Products created for China's vast surveilled and censored domestic market are increasingly popular overseas, where they are often cheaper and more appealing to consumers. Huawei, for instance, which has honed its 5G wireless technology—which will support the next generation of data-intensive, AI-powered gadgets—in China's domestic, bleeding-edge consumer market for the IoT. Many Huawei phones are bought by Chinese who have never owned a PC or other digital device, giving the company an edge in imagining and designing mobile products for developing markets that skipped over the PC era. Huawei's cheaper (and often subsidised) price points, and comparable or superior products, have made its phones a better-value purchase than the iPhone for cost-savvy consumers around the world, and its 5G infrastructure attractive for penny-pinching governments. Most are unaware, or apparently unconcerned, about censorship or surveillance.

They should be worried. According to the Soviet-style playbook that still influences Chinese security services, collecting haystacks of citizen information, by whatever means necessary, is the foundation of social control, and "stability maintenance."

The Soviet model was an analogue blend of Big Brother and big data, amassing reams of information about citizens to understand their fears, vulnerabilities and intentions, and pre-empt any challenge to the Party-State's power. China has adapted this paranoid style to the

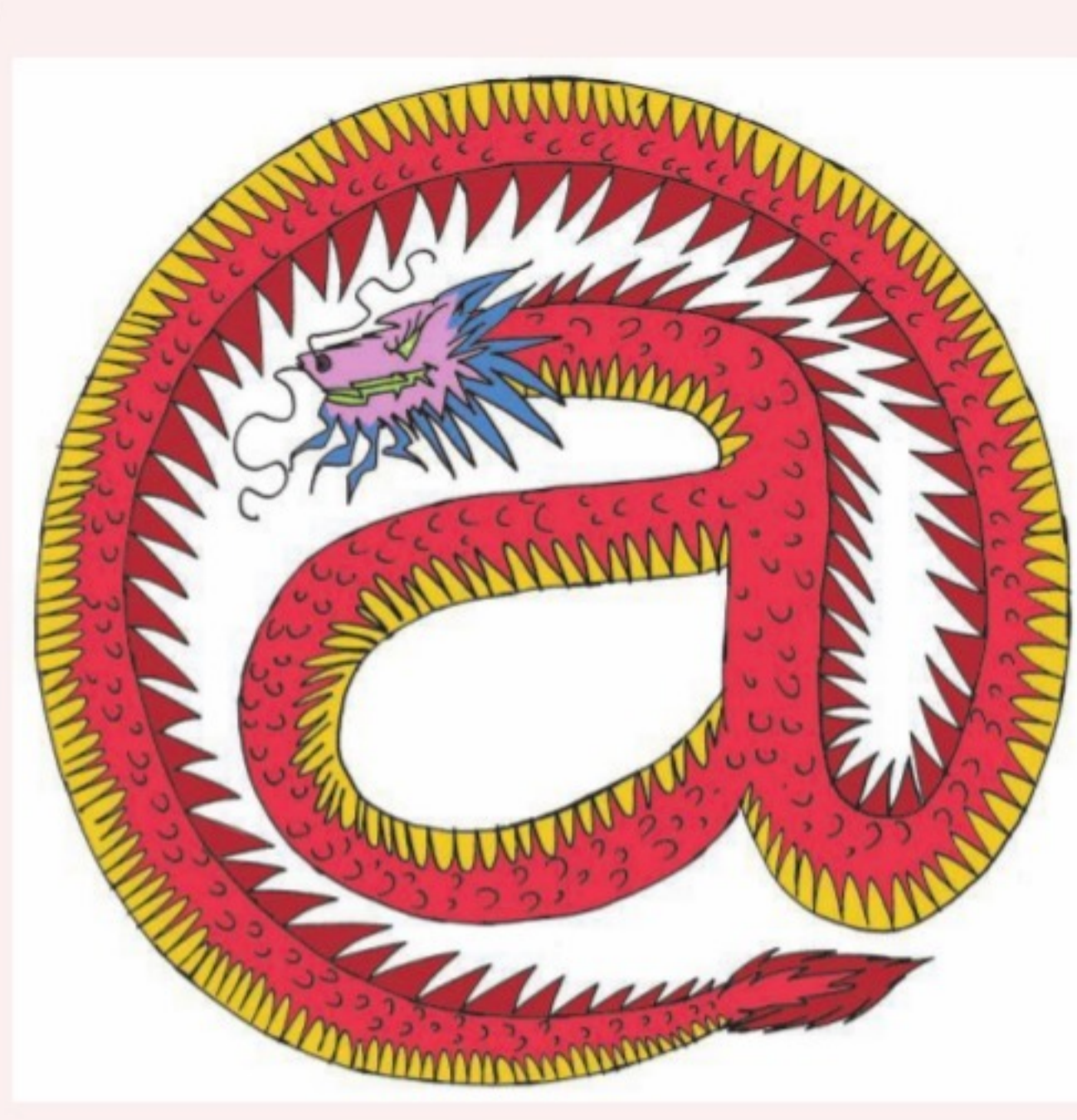


ILLUSTRATION: ROHNIT PHORE

modern tech age. Private corporations and the Communist Party's security apparatus have grown together, discovering how the same data sets can both cater to consumers and help commissars calibrate repression.

The party's instinctual contempt for privacy, married to its proactive industrial policy, can be a boon for well-connected private businesses. Many tech firms make a point of hiring the relatives of high party officials, and a vast state database of headshots might be shared with a private firm to train new facial recognition software, while the firm's trove of real-time user data might be offered to police, for a panoramic view of potential "troublemakers."

Between the Communist Party's repressive impulses, its influence over China's vast and innovative tech ecosystem, and new technology's general propensity to disrupt and surprise, it is naïve to expect that we can fully anticipate and mitigate the impact of illiberal innovations exported abroad. Even innocuous-seeming technology, when

paired with China's authoritarian impulses and state-led development model, may challenge liberal values in unexpected ways.

Consider TikTok, a social video-sharing app that last year had more downloads on the Apple app store than Instagram. TikTok fills a market niche abandoned by Vine, the American-grown short-video-sharing app shuttered by Twitter in 2017. Users can upload videos of themselves or friends lip-synching the latest pop tunes or friends operating or distorting their faces, all easily edited into a clip for other users to "like," "share" or comment on.

To China's surveillance state, a video-sharing app offers much more than your dog dancing to Drake. TikTok's domestic Chinese version, Douyin, is heavily censored and surveilled: Last year, the British cartoon Peppa Pig was purged from the platform after the authorities decided she had taken on subversive meaning.

For residents of Xinjiang, posting a video of traditional Uighur music sung in

their native language might be flagged by machine-learning algorithms, and bring a deletion and a visit from the police. In what appear to be precautionary performances of loyalty to the government, Uighur users of Douyin have recorded themselves singing pro-party songs, pointedly in Mandarin. Given the wide use of facial recognition across Xinjiang, and the potential sharing of security data sets between state agencies and private firms, Douyin's raw video data may also offer a tempting training set for machine-learning software.

To date, no evidence suggests that Chinese authorities have used their leverage over Douyin domestically to censor or surveil TikTok overseas. But given what we know about Beijing's illiberal impulses, there is a gap between what is provable beforehand, and what it is prudent to presume. The brazen lying that is normalised in China's corporate and political culture, and the meaninglessness of written rules, mean that published regulations, or guarantees by private firms and government officials, are simply not credible.

TikTok itself has already been fined by the Federal Trade Commission for a casual attitude towards privacy compliance; its heavy-handed solution, mass deletions, enraged some consumers. But the choices of ByteDance, TikTok's parent company, are rational; it fears the Communist Party more than angry tweets from tweens outside the Great Firewall.

The West's increasing technological and economic exposure to China may have unintended consequences. Over a decade ago, the singer Björk was banned from China, and muzzled within the Great Firewall, for advocating Tibetan independence during a concert in Shanghai. If, tomorrow, Björk followed up with a TikTok video pleading for Uighur rights, and the clip went viral globally, would the party be able to resist the temptation to lean on ByteDance to slow or stop it? If your face appears in the background of another person's TikTok video shot in Berlin, will it be logged using facial recognition software running in Shanghai? Those who complain that American firms like Facebook are invasive and unaccountable are unlikely to prefer China's tech giants, which are often cowed by, and collaborating with, the Party-State's opaque and irascible censorship and surveillance apparatus.

To be sure, the US has abused its own

**Ironically, the internet, which Western techno-utopians prophesied would liberalise China, may instead allow the party to indulge previously impossible fantasies of mass control. The Uighurs of Xinjiang are the first in human history to fully experience the downside of China's illiberal innovation. They are unlikely to be the last**

technological hegemony for power and profit. After World War II, much global communications infrastructure ran through wires on US soil, giving American spies ubiquitous access to the world's communications. American intelligence agencies have been credibly accused of seeding US-made electronic exports with bugs and spyware.

The critical difference with China lies not in the wiring of chips or lines of code, but in history, culture and scale. By custom, Americans trust that the contents of their snail-mail letters are protected by the Fourth Amendment; government access requires a judge to issue a warrant. American tech firms routinely stand up to the US government. Apple, for example, has developed default iOS encryptions that shield user activity from the company itself, to the frustration of the FBI. An iPhone user in Iran or Belarus benefits from Silicon Valley's civil libertarianism.

China is different. The People's Republic has always reserved the right to open its citizens' mail at any time, for any reason; there is no basis to believe its basic approach will differ because the technology is new. Ironically, the internet, which Western techno-utopians prophesied would liberalise China, may instead allow the party to indulge previously impossible fantasies of mass control. The Uighurs of Xinjiang are the first in human history to fully experience the downside of China's illiberal innovation. They are unlikely to be the last.

NYT

## DATA DRIVE

# Income tax filings fall

**F**OR THE FIRST time in the history of income tax returns, the number of returns filed dropped in FY19, to 6.68 crore from 6.74 crore in FY18, indicating the waning effect of demonetisation. Compliance has been lower in FY19 compared to the past few years as the ratio of actual filings to registered filers dropped to 79.1% in FY19 from an all-time high of 91.6% in FY18.

The new government will have to look at ways to expand the tax base as muted growth in tax filings will create further headwinds in an already stressed fiscal space. Against the revised estimates, direct tax collection in FY19 fell short by ₹50,000 crore, and in the current financial year, the budget estimates for direct tax is ₹13.8 lakh crore, a 15% rise from the revised estimates for FY19.

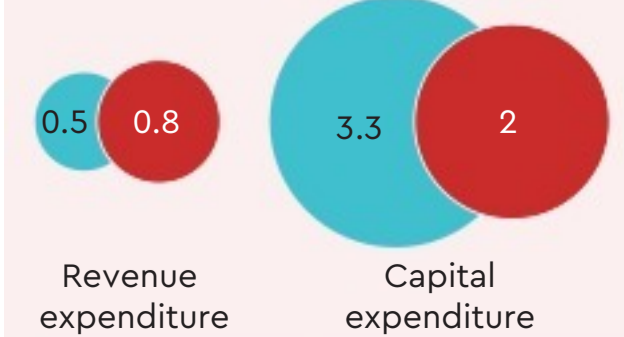
Interestingly, in indirect taxes, goods and services tax collections touched an all-time high of ₹1.13 lakh crore in March this year. Strong collections over the last two months reflect the growing compliance with indirect tax laws. The Centre has budgeted total GST collections of ₹7.6 lakh crore and states have budgeted ₹6.1 lakh crore, implying a monthly run rate of ₹1.15 lakh crore.



### Shift in income tax filings towards higher income brackets

	Mar '17	Mar '18	Mar '19
Up to 0.5	80.7	80.7	76.2
0.5 to 1	12.8	13.1	16.4
1 to 2	4.4	4.1	4.8
2 to 5	1.5	1.5	1.9
5 to 10	0.3	0.3	0.4
Above 10	0.2	0.2	0.3

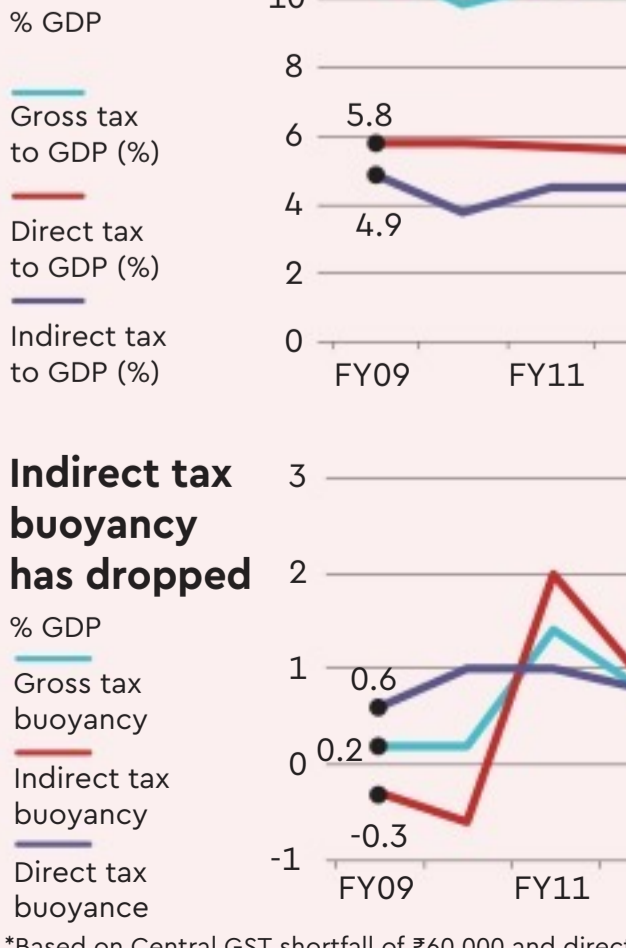
### Capital expenditure multiplier much stronger



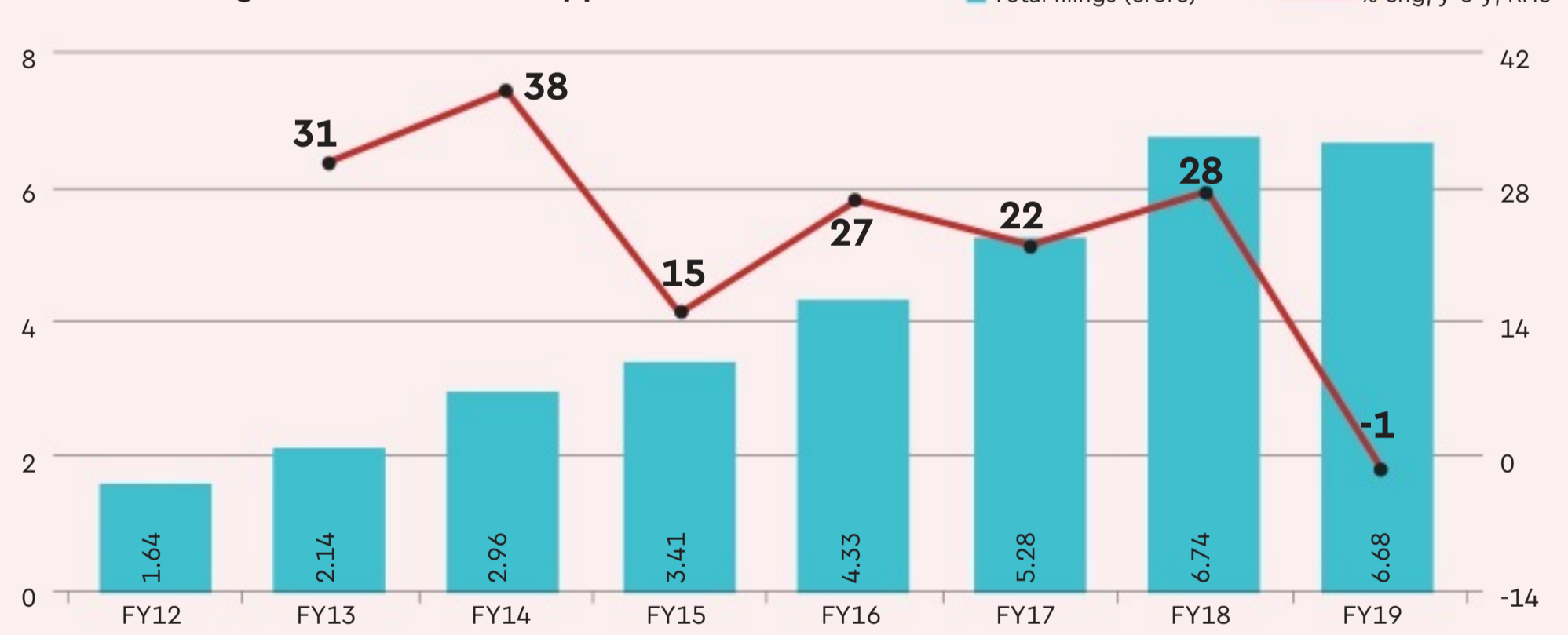
### GST collections touch record high in March this year



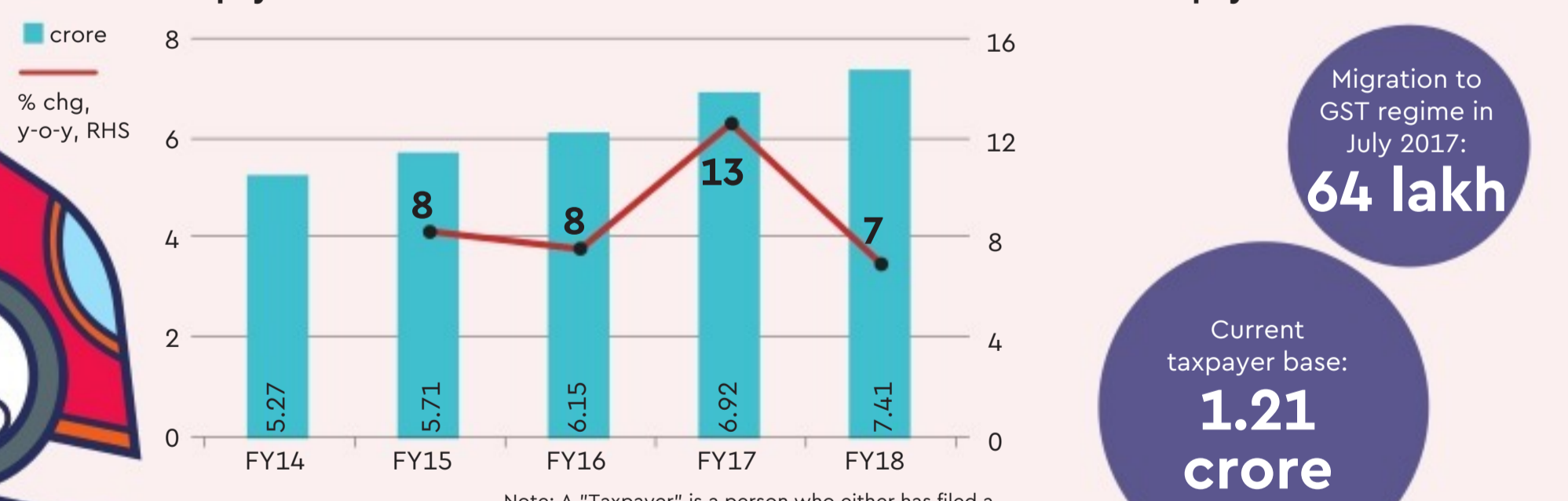
### Tax-to-GDP stagnates



### Growth in filing of e-returns has dropped in FY19



### Will total taxpayers' base increase in FY19?

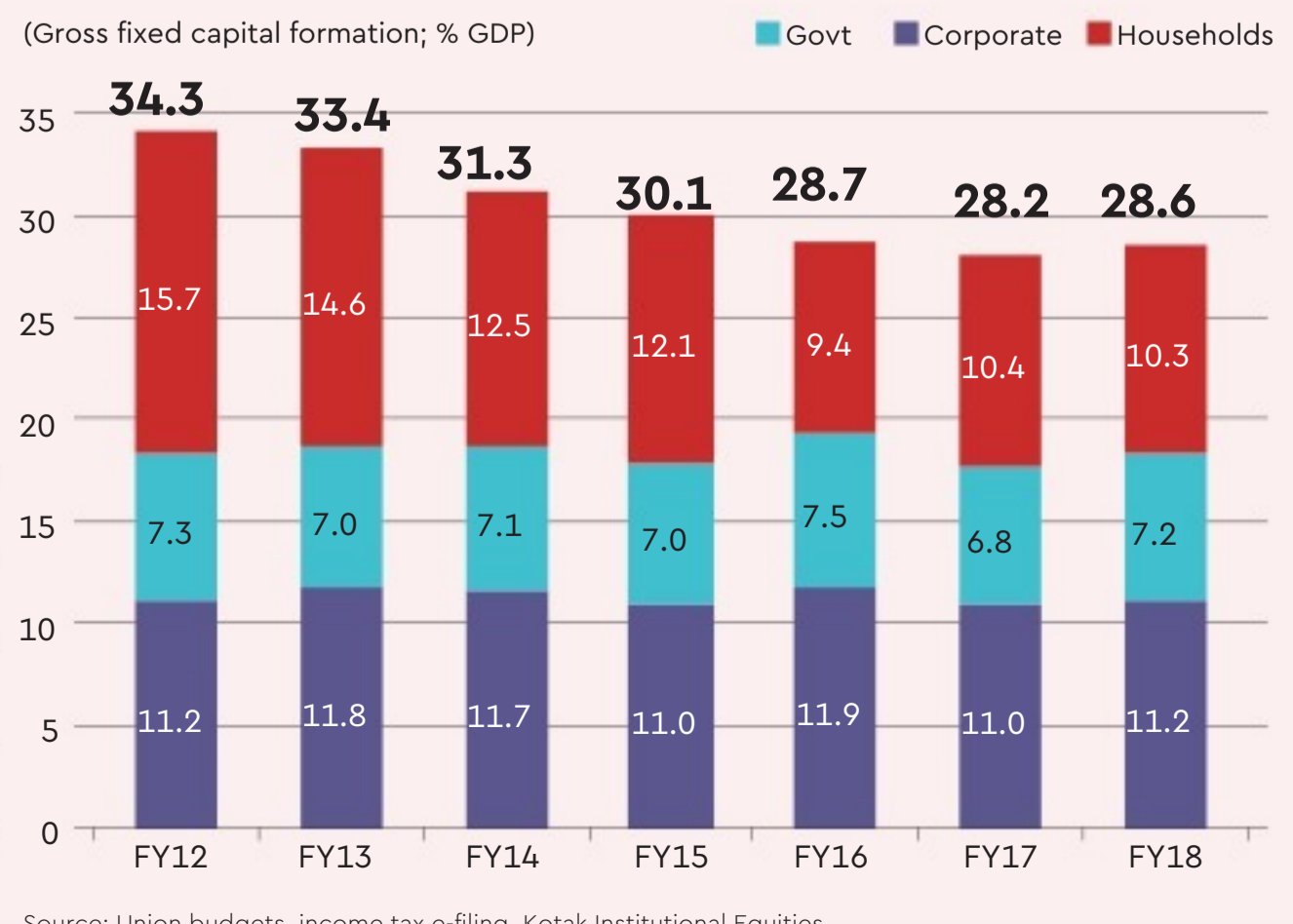


Migration to GST regime in July 2017: **64 lakh**

Current taxpayer base: **1.21 crore**

Note: A "Taxpayer" is a person who either has filed a return of income for the relevant Assessment Year (AY) or in whose case tax has been deducted at source in the relevant Financial Year but the taxpayer has not filed the return of income.

### Govt investment accounts for a small proportion of overall investments



Source: Union budgets, income tax e-filing, Kotak Institutional Equities