

This Is the Price of Government-Imposed 'Privacy'

In a tale of questionable historical validity, the British colonial government in early 20th-century India found itself confronting a fearsome pest: cobras. Though natives had long since adjusted to uneasy coexistence with the snakes, the occupying force did not take kindly to their ubiquitous presence. Seeking their eradication, authorities devised a bounty program to financially reward anyone presenting a severed cobra tail.

The program worked. Which is to say it precipitated a significant increase in severed cobra tails—the only thing the prize was truly capable of incentivizing—while also presenting enterprising individuals with a profitable opportunity: snake-breeding. Snakes need their tails neither to live, nor to reproduce, enabling a single snake to generate a stream of tails by way of countless progeny. The program had transformed the vipers into a financial instrument that would continue yielding “payments” as long as the snake could reproduce.

Confronted with abysmal failure—snakes (many tail-less) were slithering through the streets in greater numbers than before the bounty project—the authorities abandoned the scheme. The dissolution of the program encouraged snake-breeders to release their now-worthless assets into the wild, where they quickly found their way back into the city. The infamous results, now known as the “cobra effect,” depict those government interventions which generate more than the “garden variety” unintended consequence. While virtually all government interventions have *some* unintended consequences, a few positively engender the thing they were enacted to counter.

Policymakers have spawned the “cobra effect” in a host of

other contexts, including an attempt to stamp out sewer rats in colonial Vietnam and a recent effort to decimate a feral pig population at Fort Benning, Georgia. In both cases, the bounty program incentivized fraud and a swift burgeoning of the pest populations.

It's partly due to the "cobra effect" that I note with trepidation the summons for the United States to imitate Europe in its comprehensive scheme to regulate digital privacy. Since the 1995 Data Protection Directive, the EU's regime has seen several updates, notably in 2002 and in 2016, with the General Data Protection Regulation (GDPR) set to take effect in mid-2018.

Digital privacy means different things to different people. And the expansive scope of the GDPR renders sensible discussion difficult because the law contains many disparate directives. Much of the GDPR is aimed at curtailing the alleged "abuse" of non-sensitive information (an internet firm tracking a browser's activities) rather than at cybersecurity (credit card theft). Some view web privacy as a "fundamental right" on which private firms, by their surreptitious collection of data, are trampling. Ironically, these same critics often remain silent on the government's own privacy-invasive activities, which, at best, have a "chilling effect" on digital activity.

Regardless of one's stance on digital privacy, there are reasons to question whether top-down regulation is the answer to perceived privacy problems. Though the productivity-reducing impact of the European legislation has already been anticipated, I want to focus on the "cobra effect" potential of privacy law.

Commentator Geoffrey Manne warned of the Obama administration's proposed "Consumer Privacy Bill of Rights Act." Like many pieces of legislation with nice-sounding names (who could be against privacy rights?), the law carried the

potential to *increase* serious privacy threats. Though many firms don't link real-identifying info (name, credit card number) with more anonymous info (IP addresses), this bill would force firms to do just that. The rationale? So that consumers can demand to know what information has been collected and demand its deletion. For the same reason, the law might also require businesses to keep more detailed databases of their customers. This makes firms a more attractive target for would-be hackers. The cobra strikes again.

A 2005 study took advantage of the stark differences between Europe and the United States with respect to digital privacy law. Whereas Europe has an overarching digital privacy regime, the U.S. has nothing comparable. That study found that the United States is home to a flourishing industry devoted to third-party certification of firms' privacy practices. Not unlike Consumer Reports, particularly privacy-conscious firms can earn a digital "sticker," testifying to their superior privacy practices. By contrast, the United Kingdom boasts only a handful of companies offering similar services. As the authors suggest, privacy law in Europe has "crowded out" the emergence of a quality assurance (in this case, assurance of privacy) market. The results of this study suggest that it may be *easier* for privacy-sensitive U.S. consumers to identify websites that value consumer privacy. In the United Kingdom, consumers have fewer means to differentiate between the privacy practices of rival firms. Most firms simply gravitate toward the baseline privacy mandated by EU law (and some even skirt that). The result: a regulation intended to confer privacy makes it more difficult to evaluate firms' heterogenous approaches to privacy.

Lastly, under the new regulations, consumers have more opportunity to forgo supplying the information that firms seek as a "payment" in return for offering their services free of charge. Indeed, one study has shown that the 2002 updates to

the directive reduced the ability of digital firms to collect information and thus target digital advertisements to interested consumers.

Since many digital companies depend on collecting this information to sell it to advertisers, the regulation puts the squeeze on a host of firms. Less information to sell means less revenue. Firms begin looking for second-best ways of earning income. Some of them may begin charging money prices for services that were previously offered in return for information. In turn, this may lead to an increase in credit card transactions. With an increase in “sensitive” transactions, there are more opportunities for digital theft. Once again, an effort to nudge consumer-firm interaction toward privacy may result in more egregious privacy violations.

Governments are good at shifting risk in sneaky ways, but they can't legislate it out of existence. And the cobra's venomous bite provides ample reason to mistrust Big Brother's attempts to impose privacy on us all. {eoa}

Dr. Caleb Fuller is assistant professor of economics at Grove City College.

This article was originally published at . Used with permission.