MONETARY REMEDIES FOR ZERO-PRICE PRIVACY REGULATION: AN ECONOMIC PERSPECTIVE

BY ANDREW STIVERS[1]

1 Andrew Stivers is an Associate Director at NERA Economic Consulting, and former Deputy Director for Consumer Protection in the Federal Trade Commission's Bureau of Economics.

Monetary Remedies for Zero-Price Privacy Regulation: An Economic Perspective

By Andrew Stivers

Zero-price goods and services potentially create a problem for regulators interested in crafting monetary remedies that are deterrent, efficient, and inexpensive to implement in that they prevent the use of an easy proxy for injury or gain. Major privacy regulations in the EU and U.S. seem to have focused on deterrence, but in pursuit of cheap, have left any hope of efficiency to the discretion of the enforcers with little guidance on what that would mean. This paper examines regulatory choices for monetary remedies in the context of zero-price privacy and data security practices. The paper lays out the economic framework consistent with a broad range of potential harms, and argue that failing to provide any link or guidance between these remedies and the welfare effects of the practices in question will create opportunity for regulatory capture or improper political influence, and muddy the deterrent signal to potential violators.

For efficiency reasons, economists often argue that monetary remedies for competition or consumer protection law violations should be tied, at least proportionally, to the welfare effects of those violations. Here, efficiency means both accounting for the intended benefits of regulatory activity and attempting to minimize any effects on legitimate activity. A convenient, if incomplete and sometimes misleading, way to proxy for negative welfare effects is with a price premium associated with the practice in question. Zero-price goods and services remove this convenience, as price in the most plausible counterfactuals are also likely to be zero. This potentially creates a problem for regulators interested in crafting monetary remedies that are deterrent, efficient in the above sense, and inexpensive to implement. Major privacy regulations in the EU and U.S. seem to have focused on deterrence, but in pursuit of cheap, have left any hope of efficiency to the discretion of the enforcers with little guidance on what that would mean.

This paper examines regulatory choices for monetary remedies in the context of zero-price privacy and data security practices. The paper lays out the economic framework consistent with a broad range of potential harms, and argues that failing to provide any link or guidance between these remedies and the welfare effects of the practices in question will create opportunity for regulatory capture or improper political influence, muddy the deterrent signal to potential violators.

I. INJURY IN ZERO PRICE GOODS WITH PRIVACY ATTRIBUTES

The tangibility of money changing hands in the context of contested practices has provided an expedient way for courts to proxy for consumer harm in many consumer protection and competition settings. This is convenient because consumers, by purchasing something in the market, have an observable basis for injury – they gave money in exchange for some bundle of attributes – and clear attribution for that injury – they exchanged money and product directly with a specific firm.

However, when consumers do not give money when consuming some product or service, characterizing injury with respect to privacy attributes may require additional work. Establishing the basis for injury in privacy can be especially difficult, as harmful outcomes may be more removed from the data collection itself, thus requiring more work to attribute outcomes – either to the firm's practices or to specific individuals – and to estimate the monetary value of the injury associated with those outcomes. To start, the paper summarizes two general areas where consumer injury might lie when they do not pay money. Glasgow & Stomberg provide a more general discussion of injury and valuation techniques for privacy in the context of antitrust cases.[2]

First, a consumer may make non-money payments, for example in data or attention (which also generates data). Just like with money payments, transfers of data and attention are relatively easy to tie to a transaction and violative privacy practices may induce premia over compliant practices. For example, a false promise of privacy on a social media site may draw a consumer to that site, where they otherwise would not have gone. The data shared and time expended by the consumer and given to the firm could be the basis for injury, as a function of the consumer's value of those assets. Of these two, time has a relatively well-developed literature establishing its value. While there are some complications, time and attention are normal, rival, and (somewhat) excludable goods. Furthermore, while individual valuations of an increment of time varies, in general spending that increment is viewed as costly.[3] As such, there is little dispute in economics about whether misappropriated time is costly to consumers, although this does not appear to be a readily available source of legal remedy.

Harm to consumers from the misappropriation of data – independent of any feedback effects – on the other hand, is much more difficult to assess, much less well-established, and thus much more contentious. Unlike attention, which consumers often guard fiercely and trade parsimoniously in market and nonmarket settings, consumer data is more intermittently protected, and often given – or simply flows – promiscuously. That many consumers have direct preferences over those data flows is not in doubt, and with enough effort, grounded estimates of injury can be made in many cases. Substantial research over the last twenty years has consistently shown positive – if not always consistent – valuations in surveys, experiments and imputed valuation studies.[4] Recent work has validated the idea that consumers have both intrinsic (independent of feedback effects) and reactive value to that flow.[5] However, absent an explicit promise not to collect data as "payment," or an explicit statute prohibiting certain practices, it is not well established that consumers have a general right to dictate the dispersion of the data flowing from them,

2 Garrett Glasgow & Chris Stomberg "Consumer Welfare and Privacy in Antitrust Cases: An Economic Perspective" *Antitrust*, Vol. 35, No. 1, Fall 2020.

3 Hamermesh, Daniel S. "What's to know about time use?" Journal of Economic Surveys 30, no. 1 (2016): 198-203.

4 Acquisti, Alessandro, Curtis Taylor & Liad Wagman. "The economics of privacy." Journal of Economic Literature 54, no. 2 (2016): 442-92.

5 Lin, Tesary, Valuing Intrinsic and Instrumental Preferences for Privacy (June 29, 2019). Available at https://ssrn.com/abstract=3406412 or http://dx.doi.org/10.2139/ssrn.3406412.

nor is it clear that they are deprived of something of value just because that flow is captured. Unlike commercial piracy of intellectual property, for example, where there is an implicit but reasonable presumption of loss in licensing fees, it is not clear that individuals can generally monetize access to their data. As the recent *TransUnion v. Ramirez* U.S. Supreme Court decision suggests, courts struggle with how to assign value to data problems that are real, but are abstracted from concrete, individualized outcomes.[6] Finally, consumers have heterogeneous preferences for privacy that are not necessarily all pointed in the same direction. A data flow that is costly to one consumer – revelation of a credit score for someone with bad credit – could be beneficial to another – revelation of a credit score for someone with good credit. Thus, the mere presence of an increase in data collection associated with particular practices is not necessarily evidence that consumers are made worse off by that practice.

Second, there may be indirect effects that can be linked to the misappropriation or misuse of consumer data. Citron and Solove provide a comprehensive overview of possibly applicable frameworks for injury.[7] Some of these potential injuries are relatively straightforward to value and assign liability for – for example, payment account thefts or credit misappropriation from first party mishandling – but Jin & Stivers, as well as many others, have discussed the difficulties that arise even in these cases.[8] Other realized injuries, including serious, and often attributable, effects from stalking, revenge porn, or serious and unwarranted reputational effects, are difficult to value in a consistent way. This difficulty is even greater when these injuries stem largely from violation of preferences for product attributes for which there is little market data (e.g., a preference that one's publicly accessible data cannot be collected by a particular kind of private party without assent).

Gains to the firm from the contested practices may be an easier to estimate alternative to basing monetary remedies on injury. In some cases, this is based directly on a preference for using gains – in the context of attempting to invoke complete deterrence – but may also appeal to the idea that gains and injury are logically tied together, as they are in legal discussions of equitable remedies.[9] The seeming common sense basis for conflating gains and injury may apply in positive-price fraud settings, where one party is simply stealing the price of a purported good or service from the other. In a business to business context, for example, one party's failure to pay for an IP license to another can be both the injury to the owner of the IP and gains to the non-payer. Equating gains and injury makes less sense in non-fraud settings, where at least some consumers may be willing to pay some positive amount (meaning that the entire price is not injury), and the firm has expended some legitimate effort to provide that valued good (meaning that the entire price is not gain). These costs to the firm and benefit to consumers are not equivalent, meaning that not only is market price an imperfect estimate of either injury or gain, but also that a more perfect estimate of one does also not necessarily yield a better estimate of the other. The presence of persistent, unanticipated welfare effects – as in many privacy cases – further delinks any relationship between a firm revenue and injury.

In the case of zero price products, firm gains from the collecting and processing consumer data often stems from a third-party interaction – e.g. selling access to the consumers' data to someone in a different market – so the value of that third party interaction to the firm may be completely unrelated to consumers' disvalue from the collection. For example, it is hard to articulate a link between the value that some parents place on not having their children's online activities tracked, and the revenue generated from placing tracked ads in front of those children.

6 In that case, records on individuals were, in fact, incorrect. However, for many members of the class, those errors had not left the database, and thus had not seemed to have a concrete effect on the lives of those members. https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf.

7 Citron, Danielle Keats & Solove, Daniel J., Privacy Harms (February 9, 2021). GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, Available at https://ssrn.com/abstract=3782222 or http://dx.doi.org/10.2139/ssrn.3782222.

8 Jin, Ginger Zhe & Stivers, Andrew, Protecting Consumers in Privacy and Data Security: A Perspective of Information Economics (May 22, 2017). Available at https://ssrn.com/abstract=3006172 or http://dx.doi.org/10.2139/ssrn.3006172.

9 See SCOTUS opinion in *Liu v SEC* https://www.supremecourt.gov/opinions/19pdf/18-1501_8n5a.pdf.

II. REGULATORY MONETARY REMEDIES FOR PRIVACY PRACTICES

The difficulties in attribution and estimation of zero price privacy harms make tying monetary remedies to injury relatively unattractive to some policymakers because of the cost and uncertainty in imposing these remedies. However, tying monetary remedies proportionally to injury has attractive efficiency and incentive properties.[10] In the context of very complex networks of consumer data flows, where practices are often difficult to define, penalties that are tied to injury help focus firm incentives on mitigating expected harms when either the firm makes mistakes in following the law or the enforcement agency makes mistakes in applying it.[11] These incentives to reduce injury are lost when tying penalties to firm gains instead of harm.

Alternatively, penalties that are at least as large as the gains associated with the violative practices may be more likely to induce complete deterrence. A simplistic view might then suggest simply setting penalties high enough to ruin any company that was deemed to be in violation. However, in at least some contexts, regulatory language suggests a gentler approach. For example, both case law and statutory guidance for the Federal Trade Commission suggest that fines should not necessarily be higher than a firm can afford.[12] This caution may reflect a concern that both firms and regulators can make mistakes when the regulated practices are complex. To reduce exposure to those mistakes when enforcement is uncertainty, firms may have incentives to over-invest in compliance, meaning that they incur greater expense in meeting the required standards, as penalties rise. In extreme cases, firms may simply choose not to serve a market, rather than risk penalties that are disproportionate to any profit they might expect.

In practice, the most prominent data protection efforts in the U.S. and EU rely on administrative fines/civil penalties that are not linked to whether money changes hands between consumer and firm or to estimates of gain or injury. This means that neither price, nor the existence or effects of a transaction involving the consumer need to influence the monetary remedy. With respect to welfare effects more generally – injury to consumers or gain to the violating firm – only the European Union's General Data Protection Regulation ("GDPR") provides any explicit, overarching reference to market-based welfare effects in assessing fines, and even that is limited to firm gains. The GDPR provides for administrative fines that are "effective, proportionate and dissuasive,"[13] suggesting that the motivation is for deterrence, levied by some consideration toward the costs of severe punishment. The regulation offers a variety of factors that should be considered in setting the fine, including some rough proxies for harm (nature, gravity and duration of infringement, categories of data affected), the culpability and cooperativity of the firm, and:

> "any other aggravating or mitigating factor applicable to the circumstances of the case, *such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement*." [emphasis added][14]

More famously, it allows maximum administrative fines keyed to the overall size and wealth of the company – up to 2 percent of global revenue (or EUR 10,000,000, whichever is higher) for more technical violations and up to 4 percent (or EUR 20,000,000) for practices that are more fundamental to the spirit of the rule. These limits appear not to be binding in practices, for example, Google's fine from 2019 amounted to something in the range of hundredths of a percent of global revenue ($57 million vs. $160 billion).[15]

In the U.S., the Federal Trade Commission has had some success bringing consumer data cases under its general Section 5 deception and unfairness authority that parallel at least some of the rights given by the EU and the states. Where privacy was clearly a salient attribute being sold for a positive price, the Commission has been able to obtain redress. For example, the Commission obtained $100,000,000 in equitable relief from Lifelock, Inc., where the Commission alleged that the data protective services sold by the company were deceptively advertised.[16]

---

10 See Stigler, George J. "The Optimal Enforcement of Laws," Journal of Political Economy 78 no. 3 (1970) or, for a more recent overview, Polinsky, A. Mitchell & Steven Shavell. "The Economic Theory of Public Enforcement of Law." Journal of Economic Literature 38, no. 1 (2000): 45-76.

11 See, for example, the discussion of incentives in Cooper, James C., & Bruce H. Kobayashi. "An Unreasonable Solution: Rethinking the FTC's Current Approach to Data Security." George Mason Law & Economics Research Paper 20-23 (2020).

12 See 315 U.S.C. 45(m)(1)(C) "ability to pay," and *US v. Reader's Digest Ass'n Inc*, 494 F. Supp. 770 (D. Del 1980) "the defendant's ability to pay."

13 GDPR Article 83 1.

14 GDPR Article 83 2 (a)-(k).

15 See "18 Biggest GDPR Fines of 2020 and 2021 (So Far)" published May 21, 2021. Accessed July 23, 2021. https://www.tessian.com/blog/biggest-gdpr-fines-2020/. TIM data Statistica EUROPE IDATE DigWorld; 2016. H&M data Statistica Annual Report 2020. Google data Alphabet Annul Report 2020.

16 See case summary and documents at https://www.ftc.gov/enforcement/cases-proceedings/072-3069-x100023/lifelock-inc-corporation.

The Commission also obtained an $8,750,000 (reduced to roughly 10 percent for ability to pay reasons) judgement for equitable relief against Ashley Madison, a matching service for cheating spouses, where the Commission alleged both deceptive and unfair practices with respect to the privacy of user data.[17] However, application of this authority to gain equitable relief to cases where privacy as less obviously being paid for – either because of saliency or because of a zero price – seems to have been less successful. More recently, even this limited authority for equitable monetary remedy was removed by the U.S. Supreme Court's ruling against the Commission in *AMG v. FTC*.[18]

Even before that ruling, the Commission had been increasingly aggressive in using rule or order violations to trigger civil penalties. Most notably, it extracted $5 billion from Facebook for alleged violations of a 2012 FTC order relating to how it presented privacy controls to its users.[19] This judgement came after widespread coverage of Cambridge Analytica's ability to capture user data (including "friends of friends" data) without permission. The Commission took $170 million from Google/YouTube for alleged COPPA (Children's Online Privacy and Protection Act) violations. In that case YouTube was accused of capturing data from users that it should have known were likely to be children without getting parental assent, or providing any of the other COPPA requirements. For COPPA and order violations the Commission can extract up to about $43,000 per violation. Statutory guidance allowing civil penalties for violations does not mention either injury or ill-gotten gains, although there may be case law that supports consideration of injury in some contexts.[20] The Commission has not given any public accounting of its penalty calculations for these cases, so again, the deterrent signal is not clear.

Three states within the U.S. have passed comprehensive data protection statutes, California, Virginia, and Colorado. Notably, the U.S. variants provide substantially less guidance than GDPR or even U.S. federal authorities with respect to penalties. The California Consumer Privacy Act allows the state to pursue maximum civil penalties per violation of $2500 for unintentional and $7500 for intentional (or related to a minor).[21] The only guidance given is for the state to consider "good faith" on the part of the business.[22] The Colorado Privacy Act does not specify civil penalty amounts that the state can impose. However, the Colorado Consumer Protection Act (which applies to at least some of the relevant privacy practices) allows for penalties up to $20,000 per violation ($50,000 against an elderly person), with the total penalty not to exceed $500,000. The Virginia Consumer Data Protection Act also provides the state with authority to impose civil penalties up to $7,500 per violation.[23] None of the privacy statutes provide any additional guidance on calculating penalty amounts. They are all too new to have provided any useful examples of how they will be used in practice for monetary remedies.

In addition to fines or penalties, some privacy regulations also allow for private right of action. Private rights of action may in many cases serve primarily as avenues for redress. However, in the zero-price privacy space, private rights of action have also provided for recovery of statutory damages, which do not necessarily require any assessment of realized harm. For example, the GDPR allows a private right of action to recover "material, or non-material," damage with minimum statutory damage of EUR 500.[24] The question of exactly what "non-material" means seems not to have been yet resolved, but it at least opens the door to injury with zero-price products with no obvious, realized, and attributable feedback effect to the consumer. California's CCPA also allows for private rights of action and allows minimum statutory damages of between $100 and $750 per consumer per incident or the actual damages, whichever is greater in the context of a data breach. For statutory damages CCPA directs the court to consider a variety of factors, some of which could be taken as very rough proxies for injury.[25] The act also directs

17 See case summary and documents at https://www.ftc.gov/enforcement/cases-proceedings/152-3284/ashley-madison.

18 *AMG CAPITAL MANAGEMENT, LLC, ET AL. v. FEDERAL TRADE COMMISSION* https://www.supremecourt.gov/opinions/20pdf/19-508_l6gn.pdf.

19 See https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

20 15 U.S.C sec. 45(m)(1)(C). "In determining the amount of such a civil penalty, the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require." See also "Statement of Commissioner Noah Joshua Phillips, *FTC v. HyperBeard, Inc., et al* Matter No. 1923109" June 4, 2020, citing *U.S. v. Dish Network, L.L.C.*, No. 17-3111, slip op. at 16 (7th Cir. Mar. 26, 2020). See also *US v. Reader's Digest Ass'n Inc*, 494 F. Supp. 770 (D. Del 1980).

21 TITLE 1.81.5. California Consumer Privacy Act of 2018, 1798.199.90

22 TITLE 1.81.5. California Consumer Privacy Act of 2018, 1798.155.

23 Code of Virginia Title 59.1 Chapter 53 Section 59.1-584.

24 GDPR Article 832 para.1 "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."

25 Title 1.81.5 California Consumer Privacy Act of 2018, 1798.150 (a)(2) "In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth."

courts to consider the wealth of the company. If a business sells consumer data that has been opted out of, consumers can also pursue statutory damages of between $1000 and $3000 per incident, or actual damages, whichever is greater. Neither Colorado nor Virginia allow a private right of action.

For private cases brought under federal regulation in the U.S., the Supreme Court has recently increased the barrier to recovering damages when alleged injury is more difficult to tie to the practices and the individual.[26] Where statutory damages are allowed, independent of realized harm, the incentive effect of the firm is similar to civil penalties – the firm will need to assess whether the increased cost of ensuring against errors – its own, enforcers and the courts – weighs against the value of entering the market.

All these approaches of regulation bearing on privacy and consumer data sidestep the actual welfare effects of violations of the statutes. That is, they key to neither ill-gotten gains, nor to realized injury. Even the private rights of action, including federal, have called for statutory damages, with realized damages as backup. As discussed below, there are real difficulties in assigning and assessing injury with respect to privacy in general, and zero price products in particular, so this is not a surprising direction for civil penalties to take. However, as this paper argues, this may be a problem for the usual reasons.

III. DISCUSSION

The above discussion suggests that for monetary remedies on zero price privacy practices, regulators have elevated deterrence and relatively easy implementation over proportionality and efficiency. In application, the actual assessed fines could be influenced by welfare considerations, but enforcers have little guidance in how to implement proportionality, or why it might be important. Without that guidance, and without details of how enforcers calculate and apply penalties, regulators are left with several possible problems. First, lack of transparency or guidance means that penalties are more at risk of inconsistency, which could be driven by a variety of unwanted influences, including from unrelated political disfavor or regulatory capture. Second, without a process for evaluating data on harms or gains that could help reduce the cost to legitimate operations without significantly reducing deterrence, the first issue is likely exacerbated. Lastly, the deterrent signal of civil penalties that are not clearly tied to injury or gains are more difficult for potential future violators to read. While some observers may see the increased uncertainty as more likely to induce complete deterrence, this is not without cost, as discussed above. In addition, it is not clear that the penalties that are assessed can be interpreted as encouraging complete deterrence. For example, the $170 million penalty given to YouTube in its COPPA case could be viewed as small (less than 1 percent) relative to YouTube's $20 billion ad revenue from 2020, but the public does not know its relationship to the profit or revenue generated by the specific practices at issue, nor to any estimate of injury associated with those practices. Because of this, observers cannot necessarily interpret the magnitude of the compliance costs and risks associated with providing COPPA-related data services and products.

At a minimum, more explicit regulatory guidance on appropriate deterrence and efficiency related inputs to penalties would help improve the deterrence signal to potential violators and reduce inconsistency – whether driven by lack of inputs or by improper influences. But, ideally, welfare considerations would be built into the construction of monetary remedies directly, so that these penalties have the greatest chance of appropriate deterrence while being less disruptive to legitimate activity. While regulators may be concerned that binding penalties to welfare considerations will make the costs of implementing penalties prohibitive, given the difficulties discussed above, there are possible solutions. For example, regulators may be able to use reasonable presumptions about injury or gains based on available data that would be rebuttable by sound empirical analysis.

As a final note, it is important to remember that because society is still at the very beginning of this revolution in data flows, we do not have a good understanding of where it is going to take us, either in outcomes or in preferences over those outcomes, as markets, society and individuals adapt. As noted above, there is plenty of research suggesting that consumers care about their data flows, but also plenty that suggests consumer knowledge and decision making, much less regulatory expertise, are not yet mature. As consumers and policy makers gain experience, and more data is collected and analyzed on risks, preferences, and values over consumer data flows, it may be possible to better calibrate monetary remedies for efficiency. Tying regulation generally, and monetary remedies in particular to empirical estimations of injury would help make current regulation more flexible, and robust to that evolution.

26 *TRANSUNION LLC v. RAMIREZ:* https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.